目　录

第一章

基本概念

这章简单地介绍集合、映射、分类等几个基本概念，并且解释记号 $\in$，$\subset$，$\supset$，$\cap$，$\cup$，$\{\cdots\}$等的意义，作为以后各章的基础．

§1.1 集　合

数学中讨论的对象，如代数中的数，几何中的点，直线等，我们现在统统叫做**元素**，有时就简单地叫做**元**．若干个或无穷多个元的集体，叫做**集合**，或简单地叫做**集**．

我们要知道一个集，必定要知道它里面所有的元，也就是说，我们对于任意一个元，要能够判别它是否在这个集中．譬如，所有整数组成一个集，因为我们随便拿一个数来，都可以判别它是否是整数；这个集又叫做**整数集**，我们用 Z 来表示．

一个集一定有它的特性，譬如整数集中任意元，都有整数这个特性，平面上所有点组成的集与平面上所有圆组成的集都各有各的特性，因此对于一个集，我们可以用它的特性来判别任意元是否在它里面．

任意一个元 a，如果它有集合 M 的特性，也就是说，它是 M 的元时，我们就用记号

$$a \in M$$

来表示．如果它没有集合 M 的特性，也就是说，它不是 M 的元

时，我们就用

$$a \in M$$

来表示．有时，a 在 M 中我们也说 a 属于 M，或者说 M 包含 a．同样，a 不在 M 中我们也说 a 不属于 M，或者说 M 不包含 a．

一个集所包含的元假如是有穷个，就叫做**有穷集**，否则就叫做**无穷集**．一个集所包含的元的个数，叫做这集的**元数**或**浓度**．有穷集的元数当然是正整数．

集合可以用列举它的所有元来表示，譬如整数集 Z 可以写成

$$Z=\{0,\ 1,\ -1,\ 2,\ -2,\ \cdots\},$$

或

$$Z=\{\cdots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \cdots\}.$$

一般，假如 M 含有元 a，b，c，$\cdots$，我们就用记号 $M=\{a,\ b,\ c,\ \cdots\}$ 来表示．

通常一个集都含有一个以上的元，但是当它只含一个元时，这个集就与它所含的那唯一个元常常不加区别．为了叙述方便，我们更假定不包含任何元的也成为一个集，叫做**空集**．它的元数是零．譬如大于 1 而小于 2 的整数集合就是空集．

假如集合 N 中所有元都是集合 M 中元，也就是说 N 是 M 的一部分，或者说任意一个元，如果它有 N 的特性，它一定也有 M 的特性，那末 N 就叫做 M 的**子集**，M 又叫做 N 的**包含集**．我们用记号 $N\subseteq M$ 或 $M\supseteq N$ 来表示．子集与包含集的关系可以用图形(图 1.1)来说明．

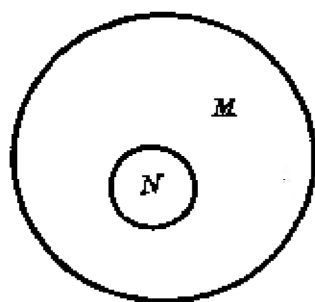


图 1.1

有穷集的子集是有穷集，无穷集的包含集又是无穷集．

为了方便，我们假定任意集都包含空集．再从 $A\subseteq B$ 及 $B\subseteq C$，我们就得到 $A\subseteq C$．

假如 M 的所有元都属于 N，同时 N 的所有元又都属于 M，即

$$M \subseteq N, \quad N \subseteq M,$$

也就是说，M 与 N 的特性完全相同时，我们就说 M 与 N **相等**，用记号

$$M = N$$

表示．假如 $N \subseteq M$，但 M，N 不相等，那末 N 就叫做 M **的真子集**，M 叫做 N **的真包含集**，用记号

$$N \subset M \text{ 或 } M \supset N$$

表示，这时 N 的所有元都属于 M，但 M 中至少有一个元不属于 N．

上面我们介绍了集合的基本概念，现在介绍它的二个结合法．

定义 1　假如 A，B 是两个集，那末属于 A 同时又属于 B 的所有元组成的集 P，叫做 A 与 B 的**交集**，用记号

$$P = A \cap B$$

表示．

于是 P 是 A，B 的子集，并且任何集只要它同时是 A，B 的子集，它一定是 P 的子集，因此 P 是包含在 A，B 中的**最大集**．关于交集的概念，我们可以用图形(图 1.2)来说明．

定义 2　假如 A，B 是两个集，那末属于 A 或者属于 B 的所

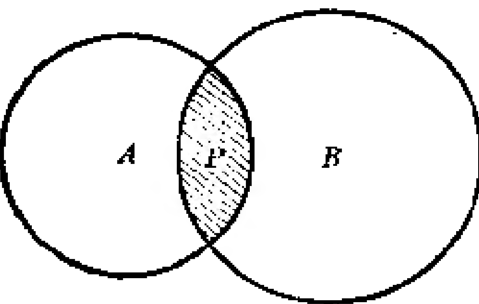


图　1.2

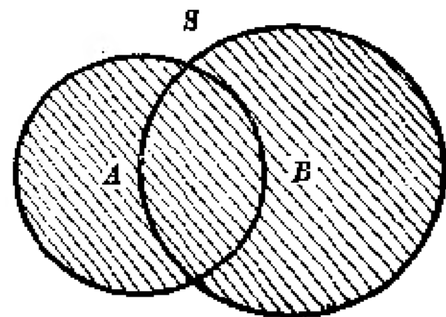


图　1.3

有元组成的集 S，叫做 A 与 B 的**并集**，用记号

$$S=A\cup B$$

表示.

于是 S 是 A, B 的包含集，并且任何集只要它同时是 A, B 的包含集，它一定也是 S 的包含集，因此 S 是包含 A, B 的**最小集**. 关于并集的概念，我们可以用图形（图 1.3）来说明.

假如 A, B, C 是三个集，显然

$$(A\cap B)\cap C=A\cap(B\cap C),\quad (A\cup B)\cup C=A\cup(B\cup C).$$

它们的交集与并集之间有下关系：

定理 $\quad A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

证明 首先因为 $B\subseteqq B\cup C$，所以 $A\cap B\subseteqq A\cap(B\cup C)$. 同样我们有 $A\cap C\subseteqq A\cap(B\cup C)$，因此

$$(A\cap B)\cup(A\cap C)\subseteqq A\cap(B\cup C).$$

再假如 $a\in A\cap(B\cup C)$，那末 $a\in A$, $a\in B\cup C$，于是 $a\in B$ 或 $a\in C$. 从前者言，$a\in A\cap B$；从后者言，$a\in A\cap C$. 因此 $a\in(A\cap B)\cup(A\cap C)$，这就是说

$$A\cap(B\cup C)\subseteqq(A\cap B)\cup(A\cap C).$$

所以定理成立.

同样我们有

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C).$$

为了区别，由元组成的集，叫做**第一层集**，把第一层集当作元组成的集，叫做**第二层集**. 第二层集又常叫做**系**.

若干个集的交集与并集可以按两个集的情形同样定义. 假定 L 是由集 A, B, C, …组成的系，我们用

$$A\cap B\cap C\cap\cdots$$

来表示 L 的交集，用

$$A\cup B\cup C\cup\cdots$$

来表示 L 的并集. 要注意的是 L 虽然是第二层集，但交集、并集却都是第一层集.

定义 3 假如 M, N 是两个集，那末属于 M 同时又不属于 N 的所有元形成的集 D，叫做 M 与 N 的差集，用记号

$$D=M-N$$

表示.

关于差集的概念，我们可以用图形(图 1.4)来说明.

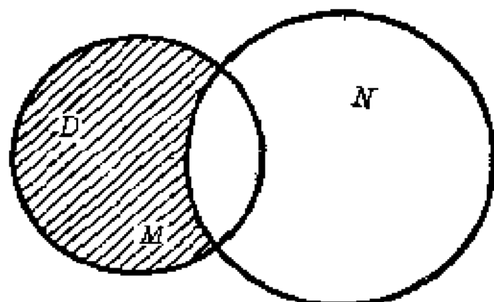


图 1.4

由定义，我们容易得知 $N\cap(M-N)$ 是空集，又

$$M=(M\cap N)\cup(M-N).$$

习 题 1.1

1. 任意两个集是否都有交集与并集?
2. 假定 $A\subseteq B$，那末 $A\cup B=$? $A\cap B=$?
3. 假定 A, B, C 是三个集，试证

(i) $$A\cup(B\cap C)=(A\cup B)\cap(A\cup C),$$

(ii) $$(A-B)\cup(B-A)=(A\cup B)-(A\cap B).$$

4. 假定 M 是元数为 n 的有穷集，L 是 M 的所有子集组成的系，试证 L 的元数是 2^n.

§1.2 映射，分类

我们知道，近世代数中集合的元是抽象的，因此，两个集合如何进行比较是一个重要问题. 映射这个概念主要用途之一就是用来解决这个问题，它是近世代数中最基本的工具.

下面是一些最基本的概念.

对于集 M 中每一个元 a，如果根据某种规则，我们可以使它

与集 N 中唯一个元对应，那末这对应叫做 M 射到 N **的映射**，那个与 a 对应的元，叫做 a 的**象**，a 又叫做它的象的**象源**．这时 M 中任意元在 N 中都有象，但 N 中任意元在 M 中不一定都有象源．如果 N 中元在 M 中不都有象源，那末这映射叫做 M 射到 N **内的映射**．如果 N 中任意元在 M 中都有象源，那末这映射叫做 M 射到 N **上的映射**．

假如 M 射到 N 的映射用 σ 来表示，那末 a 的象，我们就用 $\sigma(a)$ 来表示，有时这映射又表为 $a\to\sigma(a)$．映射这个概念与数学分析中函数的概念一致，因此 $\sigma(a)$ 又常叫做 a 的**函数**．

显然，M 射到 N 内的映射就是 M 射到 N 中某一子集上的映射．譬如在整数集 Z 中，根据自乘这个规则，把任意整数 a 与它的自乘 a^2 对应，即 $a\to a^2$，那末这对应是整数集射到自己内的映射，也是整数集射到由所有整数平方组成集上的映射．

我们知道，对于映射 σ，象源 a 固然只有唯一的象 $\sigma(a)$，但是象 $\sigma(a)$ 就不一定只有一个象源 a，它可能有一个以上的象源．任意象只有一个象源的映射，有时又叫做**一对一的映射**；不是一对一的映射，有时又叫做**多对一的映射**．假如 σ 是 M 射到 N 上的映射，B 是 N 的子集，A 是 M 中所有这样元组成的集，它们的象都在 B 中，那末 A 叫做 B 对于映射 σ 的**完全象源**．

M 射到 N 上的映射 σ，当 $a_1\neq a_2$ 时，$\sigma(a_1)\neq\sigma(a_2)$，也就是说当 $\sigma(a_1)=\sigma(a_2)$ 时，$a_1=a_2$，那末 σ 就是一对一的映射．

集合 M 射到 N 上的一对一的映射 σ 有时叫做**可逆映射**，用记号

$$a\leftrightarrow\sigma(a)$$

表示．这时 N 中元 b 的象源用 $\sigma^{-1}(b)$ 来表示．显然 $b\to\sigma^{-1}(b)$ 是 N 射到 M 上的映射，我们叫它做 σ 的**逆映射**，用记号 σ^{-1} 表示．因此，任意可逆映射都有唯一个逆映射，这逆映射也是可逆映射．

假如 σ 是可逆映射，那末它的逆映射 σ^{-1} 的逆映射就是 σ，这就是说 $(\sigma^{-1})^{-1}=\sigma$.

譬如在整数集中，我们把偶数与 0 对应，奇数与 1 对应，这样就得到整数集射到集合 $\{0, 1\}$ 上的映射，这映射是多对一的，0 的完全象源是所有偶数，1 的完全象源是所有奇数，它们都没有唯一的象源．假如我们把整数 n 与 $2n$ 对应，即 $n\to 2n$，那就得到整数集射到偶数集上的映射，这映射是一对一的，因此它是可逆映射，它的逆映射就是 $2n\to n$.

假如有一个一对一的映射把两个集 M、N 中的一个，譬如说 M，射到另一个 N 上，那末这两个集就叫做**有相等的浓度**，或**元数**．与正整数集或它的子集有相等浓度的集，叫做**可数集**．一个集如果不是可数集，就叫做**不可数集**．因此有穷集是可数集．任一可数集中元可以用正整数做标号来排列，于是任意可数集 M 可以写成

$$M=\{a_1,\ a_2,\ \cdots,\ a_n,\ \cdots\}.$$

显然整数集与偶数集有相等的浓度，因此一个集的浓度也可以与它的真子集的浓度相等，这是无穷集的一个重要性质．任意有穷集是没有这个性质的．

假定 $M=N$，那末 M 射到 N 的映射，就叫做 M **射到自己的映射**，M 射到 N 上(内)的映射，就叫做 M 射到**自己上(内)的映射**．M 射到自己上的一对一的映射，有时又叫做 M 的**变换**．对于 M 中任意元使自身与它对应，也就是说不使 M 中任意元变动，是 M 射到自己上的一个映射，叫做 M 的**恒等映射**，用 I 表示，即 $I(a)=a$．很多重要的映射都是射到自己上的映射，譬如平面上的旋转就可以看成为平面上的点集射到自己上的映射．要注意的是 M 射到自己内的映射有时是一对一的，而 M 射到自己上的映射却有时是多对一的．譬如 $n\to 2n$ 就是整数集射到自己内的一对一

的映射，$2n \to n, 2n+1 \to 2n+1$ 是整数集射到自己上的多对一的映射．

假如 σ_1, σ_2 都是 M 射到 N 上的映射，如果对于 M 中任意元 a，而 $\sigma_1(a)=\sigma_2(a)$，我们就说这两个映射**相等**，用记号 $\sigma_1=\sigma_2$ 表示．假如 σ 是 A 射到 B 上的映射，τ 是 B 射到 C 上的映射，$\sigma(a)=b$, $\tau(b)=c$, 即

$$a \to b, \quad b \to c,$$

我们容易证明，对应 $a \to c$ 就是 A 射到 C 上的映射，叫做映射 τ, σ 的**积**，用记号 $\tau\sigma$ 表示，即

$$\tau\sigma(a)=\tau(\sigma(a)).$$

这就是说，$\tau\sigma$ 是先施行 σ，后施行 τ 得到的映射．

要注意的是，虽然一个集的任意两个变换的积是存在的，但一般对于不同集的两个映射不一定有积．再映射 τ, σ 的积 $\tau\sigma$ 与 σ, τ 的积 $\sigma\tau$ 一般不是一致的．譬如 σ 是 M 射到 N 的映射，τ 是 N 射到 M 的映射，这时，$\tau\sigma$, $\sigma\tau$ 都有意义，但前者是 M 射到自己的映射，而后者则是 N 射到自己的映射，两者显然不一致．即令 $M=N$，一般 $\tau\sigma$ 与 $\sigma\tau$ 也不一定相等，象这样的例子，我们在几何上是很熟悉的．

假如 σ 是可逆映射，那末 $\sigma^{-1}\sigma(a)=a$，因此 $\sigma^{-1}\sigma=I$，这就是说 $\sigma^{-1}\sigma$ 是恒等映射．同样，$\sigma\sigma^{-1}$ 也是恒等映射．再假如 σ, τ 都是可逆映射，那末 $\tau\sigma$, $\sigma\tau$ 又都是可逆映射．显然 $\sigma^{-1}\tau^{-1}$, $\tau^{-1}\sigma^{-1}$ 就分别是它们的逆映射．

假定对于集 M 中任意两元 a, b，根据某个规则，我们可以把 a, b 与某集中唯一个元 c 对应，那末这对应，我们叫做 M 的**结合法**，有时又叫做 M 的**代数运算**．这时我们又常常说根据这结合法，可以把 a, b 结合得到元 c，因此我们又说 M 有一个结合法．譬如对于整数集 Z 中任意两数 a, b，我们命 $a+b$ 与它们对应，那末

这对应就是 Z 的结合法，它就是普通的加法．同样，对于 a, b, 我们命 $a\cdot b$ 与它们对应，这对应也是 Z 的结合法，它就是普通的乘法．

一个集，假如它具有适合某些法则的结合法，或代数运算，就叫做**代数系**．象上面所示，整数集 Z 是代数系，因为它的加法，乘法两个结合法适合交换律 $a+b=b+a$, $ab=ba$, 结合律 $a+(b+c)=(a+b)+c$, $a(bc)=(ab)c$, 分配律 $a(b+c)=ab+ac$ 等法则．近世代数的目的就是讨论某些基本代数系关于结合法的性质，也就是代数性质．因此可以说，近世代数是研究某些基本代数系的理论学科．

上面我们介绍了映射，现在再来介绍分类这个概念．

我们知道，通常我们把两个元看成为一个元，或者说两个元相等，所用的等号"="这个记号适合下面三个律：

1° 自反律：$a=a$,

2° 对称律：假如 $a=b$, 那就 $b=a$,

3° 传递律：假如 $a=b$, $b=c$, 那就 $a=c$.

并且引用等号时也只是引用了这三个律，但是适合这三个律的关系还有很多．一般来说，我们有：

定义 假如对于一个集的元，规定了一个关系～，并且可以判别其中每对元 a, b 是否有这关系 $a\sim b$；再这关系还适合自反，对称，传递三个律，即

1° $a\sim a$,

2° 假如 $a\sim b$, 那就 $b\sim a$,

3° 假如 $a\sim b$, $b\sim c$, 那就 $a\sim c$.

那末这关系，叫做这集的**等价关系**．

譬如初等几何中的三角形全等、相似都是三角形间的等价关系，但是整数集中不相等，或者大于、小于等关系都不是等价关

系．又如在有穷集 $M=\{1, 2, 4, 6, 10\}$ 中，假定两个数的和能够被 4 整除这个关系是～，即当 $4|a+b$ 时 $a\sim b$，显然对称律成立．再我们不难证明传递律也成立，但自反律不成立，因此这关系不是 M 的等价关系[1]．

在一个集中，根据某种关系或者用某个观点把某些元看成相等或同类，把某些元看成不相等或不同类，叫做**分类**．下面是分类与等价关系之间的一个重要性质．

定理 假如集 M 有一个等价关系，所有与一个元等价的元形成的集，叫做一类，那末 M 就能够分成为若干个这样没有公共元的类而无剩余．反过来，假如 M 能够分成若干个没有公共元的集而无剩余，这种集我们叫它做类，那末元素在同一类这个关系就是等价关系．

证明 定理的后半段我们容易知其成立，因此我们只要证明前半段就行了．

假定集 K_a 是 M 中所有与元 a 等价的元形成的类，那末类 K_a 中包含的元是相互等价的，这是因为从 $a\sim b$, $a\sim c$，根据对称律，传递律就得到 $b\sim c$．显然 M 中任意元必定属于这样的某一类，因此 M 可以分成这样的类而无剩余．

假如我们能够证明任意这样的两类不是相等就是没有一个公共元，那末 M 中任意一元只能在唯一类，因此定理的前半段就告成立．

假定两类 K_a, K_b 有一个公共元 c，那末 $a\sim c$, $b\sim c$，因此 $b\sim a$．如果元 $x\in K_a$，因为 $a\sim x$，所以 $b\sim x$，于是 $x\in K_b$．因此 $K_a\subseteq K_b$．同样我们可以证明 $K_b\subseteq K_a$，所以 $K_a=K_b$．这就是说，任意两类如果不相等，那末它们就没有一个公共元，于是定理的前半段成立，因此定理得证．

于是我们得知一个集，如果有一个等价关系，它就有一种分

类．反过来，如果它有一种分类，它就有一个等价关系．

假如 n 是正整数，在整数集 Z 中，两数 a, b 的差 $a-b$ 如果能够用 n 整除，即 $n|(a-b)$ 时，叫做 a 与 b 关于模 n **同余**，用记号

$$a\equiv b(\mathrm{mod}\ n) \quad 或 \quad a\equiv b(n)$$

表示，有时又简写成 $a\equiv b$．显然 $a\equiv a$，并且我们容易证明：假如 $a\equiv b$，那末 $b\equiv a$．再假如 $a\equiv b$，$b\equiv c$，那末 $a\equiv c$，所以它是等价关系．于是对这个关系，整数集 Z 有一个分类，a 所在的类是所有形状象 $a+kn$（k 是任意整数）的数形成的集，叫做 **a 关于 n 的同余类**，我们用 $\bar{a}$ 表示，因此 Z 可以分成为 n 个同余类

$$\bar{0},\ \bar{1},\ \cdots,\ \overline{n-1}.$$

这是因为关于模 n，任意一整数必定与 $0, 1, \cdots, n-1$ 中某一数同余，并且 $0, 1, \cdots, n-1$ 中任意两数都不同余．当 $n=1$ 时，整个整数集 Z 成为一类，当 $n=2$ 时，Z 就分成为两类，一类是所有偶数形成的偶数类，一类是所有奇数形成的奇数类．任意元只与自身同余，并且相异的元都不同余的同余叫做**零同余**．因此 Z 自身可以看成是根据零同余的分类，它的每个同余类只有一个元．

上面是为了叙述方便，假定 $n>0$，其实 $n<0$ 时也是同样成立的，这时整数集 Z 可以分成 $|n|$ 个同余类．

习 题 1.2

1．假如 $a\equiv b(n)$，$c\equiv d(n)$，那末

$$a+c\equiv b+d(n), \quad a-c\equiv b-d(n),$$
$$ma\equiv mb(n), \quad ac\equiv bd(n).$$

2．试就 $n=-5$ 时，把整数集 Z 分类．

3．假如 σ 是 A 射到 B 的映射，τ 是 B 射到 A 上的映射，如果 $\sigma\tau=I$，那末 σ 是 τ 的逆映射．

4．假如 σ 是 M 射到 N 上的映射，A, B 分别是 M, N 的子集，试证 $\sigma(A)$ 的完全象源包含 A，而 B 的完全象源的象就是 B．

5. 有人说从对称律和传递律可以推出自反律，因此自反律可以不要，他的理由是从 $a \sim b$，由对称律得 $b \sim a$，再由传递律便得 $a \sim a$，你的意见如何？

6. 等价三个律可以改成为(1) $a \sim a$，(2)如果 $a \sim b, a \sim c$，那末 $b \sim c$。为什么？

§1.3 自然数，数学归纳法

依照发展的过程来讲，人类首先知道的数是正整数，也就是自然数

$$1, 2, 3, 4, 5, \cdots,$$

它们形成的正整数集又叫做**自然数集**. 在这节我们不叙述以它的基本性质为特征的公理[2]，只叙述它的一些基本性质，目的在介绍数学归纳法的证法和定义，以备以后引用.

一个集，假如有一个叫做某元在某元前面的顺序关系，元 a 在元 b 前面我们就说 a 小于 b，或者 b 大于 a，用记号 $a<b$ 或 $b>a$ 来表示，如果这关系又满足下面两个条件：

1° 对于任意两元 a, b，下面的关系必定有一而且只有一成立：

$$a=b, \ a<b, \ a>b;$$

2° 对于三元 a, b, c，从 $a<b$, $b<c$，就有 $a<c$，

那末这集就叫做**有序集**. 空集认为是有序集. 自然数集依数大小的顺序是有序集，这性质有时又叫做**自然数的有序性**.

再自然数集是无穷集，即它的元数不是自然数. 假如它里面的数依大小的顺序排，那末在任意一数的后面还有数.

下面是自然数集的另一基本性质，这性质有时又叫做自然数的最小性.

定理 1 在自然数集的任一非空子集 M 中，必定有一个最小

数，也就是说在集 M 中有不大于其他任意数的数.

证明 因为 M 非空，所以在 M 中可以取一数 n，显然，M 中所有不大于 n 的数形成的非空集 $N\subseteq M$. 如果 N 中有最小数，那末这最小数就是 M 的最小数，但从 1 到 n 只有 n 个自然数，于是 N 中所含的数最多只有 n 个，所以 N 有最小数，因此定理成立.

根据这性质我们可以推得下面重要定理，它是数学归纳法原理的依据.

定理 2 假定 M 是由自然数形成的集，如果它含有 1，并且当它含有数 $n-1$ 时，也含有数 n，那末它含所有的自然数，即 M 是自然数集.

证明 假定 N 是所有不属于 M 的自然数形成的集，那末 $1\overline{\in}N$；如果 N 非空，由上面的定理得知 N 中必定有一个最小数 c，因为 $c\overline{\in}M$，所以 $c\neq1$，因此 $c-1$ 是自然数. 但 c 是 N 中最小数，所以 $c-1\in M$，于是由假设，$c\in M$. 这与上面的假设矛盾. 因此 N 是空集，也就是说，所有自然数都在 M 中，所以定理得证.

于是我们得知，为了要证明一个命题对于所有自然数都是真的，我们只要证明两件事，首先证明它对于 1 是真的，再假定这命题对于自然数 $n-1$ 是真的时，进而证明它对于自然数 n 也是真的就行了. 这就是普通所谓的数学归纳法. 此外，数学归纳法还有下面另一形式.

为了要证明一个命题对于所有的自然数都是真的，我们只要证明它对于 1 是真的，并且假定它对于所有小于 n 的自然数都是真的时，再证明它对于自然数 n 也是真的就行了. 这形式在应用上有时比上面的方便.

譬如，任意一笔大于 7 元的整数付款可以用 3 元及 5 元票面的钞票支付，这一事实可以用数学归纳法验证如下：显然，8 元的付款可以用一张 3 元及一张 5 元的钞票支付，这就是说，当 $n=1$，

即 $1+7=8$ 时，这事实是真的；假定小于 n 时这事实是真的，因为

$$n+7=[(n-3)+7]+3,$$

所以当 n 时这事实也是真的，因此对于任意 n 这事实都是真的，即任意 $n+7$ 元的付款都可以用 3 元及 5 元的钞票支付.

再有许多定义也可以根据归纳法的原理来规定，这就是说，一个定义对于所有的自然数都规定好了，只要根据两件事，首先我们对于数 1 规定这定义，其次假定这定义对于自然数 $n-1$（或是小于 n 的所有自然数）已经规定好了，再规定它对于自然数 n 的意义就行了.

譬如假定一个集有一个乘法的结合法，其中任意 m 个元 a_1, a_2, $\cdots$, a_m 的乘积

$$\prod_{i=1}^{n} a_i = a_1 a_2 \cdots a_n,$$

我们可以根据归纳法这样来规定它的意义：

$$\prod_{i=1}^{1} a_i = a_1, \quad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n.$$

习 题 1.3

1. 试用归纳法证明对于任意自然数 n,

$$4^{n+1}-3n-4$$

必定是 9 的倍数.

2. 试用归纳法原理规定 a^n 的意义，这里 n 是自然数.

参考文献

[1] R. A. Rosenbaum, Remark on Equivalence relation, Amer. Math. Monthly, 62 (1955), 650.

[2] N. B. 勃罗斯库列亚柯夫著，数与多项式（吴品三译），第三章（高等教育出版社）.

第二章

群

这章简单地介绍群的基本概念，主要是说明群、子群、同构、同态、正规子群、商群等的意义，以及它们的基本性质．在第五章我们还要进一步讨论一些比较复杂的重要性质．

§2.1 群的概念

在数学各部门及它的应用中，很多代数系是只有一种结合法的，譬如后面所述的变换的集合就是这样．在只有一种结合法的代数系中，最重要的就是群，它的运算法则与数的运算法则类似，并且有非常广泛的应用，是近世代数中最基本的概念．

定义 一个集 G，假如它不是空集，并且满足下面四个条件，就叫做群：

1° G 有一个闭合的结合法，这就是说，G 中任意两元 a, b 的结合 c 仍然是 G 中元．结合法通常写成乘法，这时 c 又叫做 a, b 的积，我们用记号

$$a\cdot b=c \text{ 或 } ab=c$$

来表示．要注意的是积 ab 虽然是由 a, b 一意决定的，但一般它还与 a, b 的顺序有关，也就是说 ab 不一定等于 ba．

2° G 的结合法适合结合律，也就是说，对于 G 中任意三元 a, b, c，我们有

$$(ab)c=a(bc).$$

3° 对于 G 中任意元 a, 在 G 中(最少)有一个(左)**单位元** e, 满足

$$ea=a.$$

4° 对于 G 中任意元 a, 在 G 中(最少)有一个满足

$$a^{-1}a=e$$

的(左)**逆元** a^{-1}, 这里 e 就是上面的(左)单位元.

一个非空集, 假如它满足上面的条件 1°, 也就是说, 它有一个闭合的结合法时, 我们就叫它做**乘集**. 假如它满足上面 1°, 2° 两个条件, 我们又叫它做**半群**. 半群也是一个重要概念.

一个群, 假如它的结合法还满足交换律:

$$ab=ba,$$

就叫做**可换群**, 或**阿贝耳**(N. H. Abel, 1802～1829)**群**.

群这个概念概括了很多代数系, 为了对这概念有较深入的了解, 下面给出一些例.

譬如所有正有理数, 结合法是通常的乘法形成一个群, 它的单位元是 1. 有理数集 Q 对于加法成群, 单位元是 0. 但对于乘法只成为半群, 而不能成为群, 因为零没有逆元. 同样, 整数集 Z 对加法成群, 又整数 1, -1 或者单独的一个整数 1, 对乘法都成群, 这些都是可换群. 由 1 个元形成的群, 叫做**单位元群**, 元数是有穷的群叫做**有穷群**, 否则就叫做**无穷群**.

下面我们再给出两类重要的群, 它的元并不是数.

由实数组成的所有 n 级满秩矩阵对乘法形成为群, 叫做 K 上的 n 级线性群, 或简称**线性群**, 用 $GL(n, K)$ 表示, 这里 K 是实数集. 线性群的单位元是对角线上元都是 1 其余都是 0 的单位矩阵.

在空间, 绕一个固定点的所有旋转形成一个群, 叫做**旋转群**.

这是因为两个旋转 s, t 顺次施行的结果仍然是一个绕那个固定点的旋转. 假如我们把先施行 t 再施行 s 所得到的旋转, 叫做 s, t 的积, 用 $s\cdot t$ 或 st 表示, 那末结合律显然成立. 恒等旋转就是单位元. 一个旋转的逆就是与原旋转相反的旋转. 从几何的直觉我们很容易得知 st 不一定是 ts, 因此旋转群不一定是阿贝耳群.

假如空间中所有点的集合用 M 表示, 那末绕一个固定点的旋转, 显然是 M 射到自己上的可逆映射, 也就是 M 的变换. 但变换不一定是旋转, 如果把旋转换成更广泛的变换, 我们要问, M 的所有变换是否也象上面旋转一样能够形成为群?

因为变换是可逆映射, 由 §1.2 我们得知, 任意两个变换 s, t 的积 st 仍然是一个变换, 它是先施行变换 t, 再施行变换 s 所得到的变换. 假如 a 是施行的对象, 那就有

$$st(a)=s(t(a)).$$

要证明结合律 $(rs)t=r(st)$, 我们只要把两边的变换同时施行到对象 a 上面, 我们就有

$$(rs)t(a)=(rs)(t(a))=r(s(t(a))),$$
$$r(st)(a)=r(st(a))=r(s(t(a))),$$

因此结合律成立. 恒等变换 I 是把每个施行对象仍然变成自己的映射, 即

$$I(a)=a,$$

因此对于任意变换 s, 我们有 $Is=s$, 所以恒等变换具有群的单位元的性质. 任意变换 s 都有逆变换 s^{-1}, 它是把 $s(a)$ 变成为 a 的映射, 因此 $s^{-1}s=I$. 从上面看来, 集 M 的所有变换满足群的四个条件, 所以所有这些变换形成为群, 叫做集 M 的**变换群**. 显然它不是可换群. 假如 M 是元数为 n 的有穷集, 那末这个群也叫做 **n 个文字上的对称群**, 或 **n 次对称群**, 或者简称为**对称群**, 用 S_n 表示. 也就是说, n 个文字上的所有变换形成的群就是对称群 S_n. 我们容

易知道，对称群 S_n 的元数是 $n!$. 所以 S_n 是有穷群，并且不是可换群。

当 M 是有穷集时，它的变换有时又叫做排列. 对于排列，也就是对于对称群的元，下面有一个简明的表示法.

假如 M 是元数为 n 的有穷集，它的元记成 1, 2, …, n, 那末它的排列 s 可以用式子表示如下：

$$s=\begin{pmatrix} 1 & 2 & \cdots & n \\ s(1) & s(2) & \cdots & s(n) \end{pmatrix},$$

式中 $s(i)$ 就是它上面 i 的象. 譬如，

$$s=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

是{1, 2, 3, 4}的一个排列，它把 1 换成 2, 2 换成 4, 3 不动，4 换成 1. 再我们容易知道，

$$s^{-1}=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

又假定

$$t=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

那末

$$st=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix},\quad ts=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

对称群在代数中是非常重要的. 从历史来说，研究群首先是研究对称群，群的抽象化是自弗罗宾纽斯(G. Frobenius, 1849～1917)开始的. 在第六章，我们得知对称群的概念首先是伽罗瓦(E. Galois, 1811～1832)[1]建立的，他创造这概念来证明 4 次以上的一般多项式不能够用根号解出. 此外，由后面 §2.4 我们还得知，一个有穷群可以看成是对称群的子群，因此，假如对称群研究清楚了，有穷群也就研究清楚了.

上面给出了群的一些例子，现在我们再从群的定义出发来讨

论群的基本性质.

从群定义中条件 2°,我们得知任意三元 a, b, c 的乘积,由它们自身及它们的顺序一意决定,与结合的先后也就是与所加的"括弧"无关,对于任意 n 个元的积也是如此.

定理 1 群 G 中任意 n 个元 $a_1, a_2, \cdots, a_n$ 的乘积由它们自身及它们的顺序一意决定.

证明 我们用归纳法来证明. 当 $n=3$ 时,就是群定义中的条件 2°. 现在假定元数小于 n 时定理成立,来证明元数是 n 时定理也成立.

n 个元依 $a_1, a_2, \cdots, a_n$ 的顺序的乘积不外下列各种形式:

$$(a_1)\cdot(a_2\cdot a_3\cdots a_n),$$
$$(a_1\cdot a_2)\cdot(a_3\cdots a_n),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(a_1\cdot a_2\cdots a_{n-1})\cdot(a_n).$$

但其中任意一种

$$\begin{aligned}(a_1\cdot a_2\cdots a_m)(a_{m+1}\cdots a_n) &= (a_1\cdot(a_2\cdots a_m))\cdot(a_{m+1}\cdots a_n)\\ &= (a_1)\cdot((a_2\cdots a_m)\cdot(a_{m+1}\cdots a_n))\\ &= (a_1)\cdot(a_2\cdots a_n),\end{aligned}$$

这就是说,它们都与第一种一致,所以它们的乘积与所加的括弧无关,因此定理成立.

假如 G 是可换群,那末 $a_1, a_2, \cdots, a_n$ 的乘积由它们自身就唯一决定,与它们的顺序无关.

于是为了方便,n 个元 $a_1, a_2, \cdots, a_n$ 的乘积,我们就用 $a_1a_2\cdots a_n$ 表示,不另加括弧. 此外,与普通代数学中一样,我们又有

$$\underbrace{a\cdots a}_{n\text{个}}=a^n,\ \underbrace{a^{-1}\cdots a^{-1}}_{n\text{个}}=a^{-n},\ a^0=e,\ a^1=a.$$

从群定义中 3°, 4° 两条件,我们有 $a^{-1}aa^{-1}=ea^{-1}=a^{-1}$; 用

a^{-1} 的(左)逆元左乘就得到 $eaa^{-1}=e$, 即

$$aa^{-1}=e.$$

也就是说，左逆元同时又是**右逆元**，因此我们又叫 a^{-1} 做 a 的**逆元**. 再因为

$$ae=aa^{-1}a=ea=a,$$

也就是说，左单位元同时又是**右单位元**，因此我们又叫 e 做**单位元**.

群的单位元只有唯一的一个，这是因为，假如 e_1, e_2 都是单位元，那就有

$$e_1e_2=e_2=e_1.$$

元 a 的逆元也只有唯一的一个，这是因为，假如 b, c 都是 a 的逆元，那末 $ba=e$, $ca=e$, 因为 $ac=e$, 所以

$$b=bac=ec=c.$$

显然，元 a 又是它的逆元 a^{-1} 的逆元，即

$$(a^{-1})^{-1}=a.$$

关于两个元乘积的逆元，我们有下面的计算规则:

$$(ab)^{-1}=b^{-1}a^{-1},$$

这是因为，$(b^{-1}a^{-1})ab=b^{-1}(a^{-1}a)b=b^{-1}b=e$.

假定 a, b 是群 G 的元，那末方程 $ax=b$ 与 $ya=b$ 在 G 中都只有唯一个解，这是因为

$$a(a^{-1}b)=(aa^{-1})b=eb=b,$$

$$(ba^{-1})a=b(a^{-1}a)=be=b.$$

所以 $x=a^{-1}b$, $y=ba^{-1}$ 分别是它们的解. 显然，它们的解都是唯一的.

我们又常常说 $a^{-1}b$ 是 a 左除 b 的商，ba^{-1} 是 a 右除 b 的商. 因为乘法与因子的顺序有关，所以 a 左除 b 与 a 右除 b, 它们的商一般不是一致的. 于是在群中，乘法这种运算是有逆运算的，也就

是说，在群中除了乘法运算外，还有它的逆运算除法这种运算，并且对于除法来说，它也与乘法一样是闭合的.

假定 a, b, b' 是群 G 的元，并且 $ab=ab'$ 或 $ba=b'a$，那就有 $b=b'$. 这是因为，用 a^{-1} 左乘 $ab=ab'$ 的两边或用 a^{-1} 右乘 $ba=b'a$ 的两边，就得到 $b=b'$. 因此群的结合法又是适合消去律的.

下面我们来讨论群形成的条件.

显然，群定义中 3°, 4° 两个条件可以引用(右)单位元及(右)逆元而改成为 $ae=a, aa^{-1}=e$ 的形式，但是不可改为 $ae=a, a^{-1}a=e$. 此外，这两个条件还可以用另外的形式来表达.

定理 2 群定义中 3°, 4° 两个条件，可以用对除法是闭合的，也就是说，对于群中任意元 a, b，方程 $ax=b, ya=b$ 在群中有唯一个解这条件来代替.

证明 我们只要用群定义中 1°, 2° 两条件与对除法是闭合的这一条件能够证明群定义中 3°, 4° 两条件就行了.

假定 c 是群中元，e 是方程 $xc=c$ 的解，即 $ec=c$. 如果 a 是群中任意元，并且 $cy=a$，那末由 $ecy=cy$，即得

$$ea=a.$$

因此群定义中条件 3° 成立. 至于条件 4°，从 $xa=e$ 的可解性就可以推出来，所以定理得证.

由上面的证明，我们得知群中一元如果与群中某元相乘，其积仍然是某元，那末它就是单位元. 又，一个集，假如它对于乘法及它的逆运算除法都是闭合的，并且适合乘法的结合律，那末它就成为群.

定理 3 假如 G 是有穷集，那末它成群所需要的除法是闭合的这条件又可以用消去律来代替.

证明 假定 $G=\{a_1, a_2, \cdots, a_n\}$，$a$ 是 G 中任意元，那末 $\{aa_1, aa_2, \cdots, aa_n\}$ 是 G 的子集，但这 n 个元彼此互异，因为假如 $aa_i=$

aa_j，由消去律就得到 $a_i=a_j$，这与假设不合，所以 $G=\{aa_1, aa_2, \cdots, aa_n\}$. 因此 G 中任意元 b 可以写成 $b=aa_i$ 的形式，所以 $x=a_i$ 是方程 $ax=b$ 在 G 中的解. 同样，我们可以证明 $b=xa$ 在 G 中也有解，因此定理成立.

于是我们得知适合消去律的有穷半群是一个群.

群的很多性质可以用来作为它的定义，因此群可以有很多不同的定义. 罗伦茨(P. Lorenzen)曾举了40个以上的定义，其中有不用乘法而用除法来定义的，读者如有兴趣，可参考本章末的文献[3].

我们容易知道，一个乘集或一个群，假如其中任意两元的积已经知道，那末这乘集或这群也就完全知道. 假如乘集 $G=\{a_1, a_2, \cdots, a_n, \cdots\}$，卡莱(A. Cayley, 1821～1895)用下面的表来表示 G 中任意两元的结合，叫做**乘法表**，当 G 是群时，这表又叫做**群表**.

	a_1	$\cdots$	a_n	$\cdots$
a_1	a_1a_1	$\cdots$	a_1a_n	$\cdots$
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	a_na_1	$\cdots$	a_na_n	$\cdots$
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

譬如群 $G=\{e, a, b\}$ 中元的结合法为

$$ee=e,\ ea=ae=a,\ eb=be=b,$$
$$aa=b,\ bb=a,\ ab=ba=e.$$

那末它的群表就是

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

从乘法表看元素间的结合非常明显，因此我们给出一个群时，常常就给出它的群表．在群表的每行每列中，群的任意元必定出现一次而且也只出现一次，这是因为在群中消去法是成立的．可换群并且只有可换群才有关于主对角线对称的群表．

当群 G 的结合法满足交换律时，也就是说 G 是可换群时，我们常常把结合法写成加法，积 ab 就写成和 $a+b$，这时 G 又叫做**加群**，有时也叫做**模**．单位元写成 0，叫做**零元**，元 a 的逆元写成 $-a$，叫做**负** a．即

$$0+a=a, \quad -a+a=0.$$

再

$$\underbrace{a+\cdots+a}_{n\text{个}}=na, \quad \underbrace{(-a)+\cdots+(-a)}_{n\text{个}}=-na.$$

并且我们又常常把 $a+(-b)$ 写成 $a-b$，叫做 a 减 b，因此 $-(a-b)=b-a$．特别当模的元是数时，我们又常常把它叫做**数模**，因此有理数集 Q，整数集 Z 都是数模．

习 题 2.1

1．假如{1, 2, 3, 4}的乘法表是

	1	2	3	4
1	2	1	4	3
2	4	2	3	1
3	1	3	2	4
4	3	4	1	2

它们是否成为群？假如不成为群，结合律是否成立？有无单位元？

2．试证下面四个矩阵对于乘法成群：

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

3．试证下面六个分数：

$$r, \quad \frac{1}{r}, \quad 1-r, \quad \frac{1}{1-r}, \quad \frac{r-1}{r}, \quad \frac{r}{r-1}$$

成群，这时两个分数的结合法是把第二个分数代入第一个分数中的 r 得到的结果。

4．试求 s^2, t^2, st, ts, tst^{-1}, sts^{-1}，假如

$$s=\begin{pmatrix} a & b & c & d & e \\ b & e & a & d & c \end{pmatrix},\quad t=\begin{pmatrix} a & b & c & d & e \\ b & c & a & e & d \end{pmatrix}.$$

5．试求 3 个文字上的对称群 S_3 的群表．

6．假如 a, b 是群中两元，如果 $(ab)^2=a^2b^2$，试证 $ab=ba$．

7．假如 G 是群，如果其中任意元的逆元就是它自身，试证 G 是可换群．

8．试证在任意元数大于 2 的非可换群中，存在满足 $ab=ba$ 两个异于单位元的元 a, b．

9．假定 G 是群，a 是 G 中一元，试证映射 $\sigma_a(g)=ag$（或 ga），$g\in G$，是 G 的变换，并且 G 的所有这样的变换形成一个群．

10．假定 G 是非空集合，它有一个叫做除法的闭合的结合法 a/b，并且

$$1^\circ\ a/a=b/b=e,\quad 2^\circ\ a/(b/b)=a,\quad 3^\circ\ (a/c)/(b/c)=a/b,$$

试证 G 对乘法 $ab=ab^{-1}$，$b^{-1}=e/b$ 成群，其中 $a/a=e$ 是单位元，$e/a=a^{-1}$ 是 a 的逆元．

§2.2 子 群

在研究一个群的构造时，也就是说，整个地来看群中元素间的关系时，当然需要考虑它的子群．群的全部内容大都与子群有关，子群是一个重要概念．

定义 一个群 G 的非空子集 H，假如对于 G 的结合法形成为群，就叫做 G 的**子群**．

譬如整数集对加法形成的群是有理数集对加法形成的群的子群，但 1，-1 对乘法形成的群不是有理数集对加法形成的群的子群，因为它们的结合法不一致．

群可以看成自身的子群，异于自身的子群，叫做**真子群**．任一群有只由单位元形成的单位元群做它的子群．一个群的任意多个

子群的交集仍然是一个子群，但是任意两个子群的并集却不一定成群.

假如 H 是 G 的子群，显然 H 的单位元就是 G 的单位元，H 中元 a 的逆元也就是 a 在 G 中的逆元.

下面我们首先讨论子集形成子群的条件.

定理 1 群 G 的非空子集 H 成为子群的必要充分条件是:

$1°$ 假如 H 包含元 a, b, 那末它也包含它们的积 ab,

$2°$ 假如 H 包含 a, 那末它也包含 a 的逆 a^{-1}.

证明 因为必要性显然成立，现在我们只要证明充分性.

上面的条件 $1°$ 就是群定义的条件 $1°$，结合律在 G 中成立，当然在 H 中也同样成立. 再根据上面的条件 $2°$，我们又得知假如 H 包含 a，它也包含 a^{-1}，因此 H 包含 $a^{-1}a=e$，于是 H 成群，所以定理成立.

上面两个条件，我们把它并合成为一个，就得到

定理 2 群 G 的非空子集 H 成为子群的必要充分条件是：假如 H 包含 a, b，那末 H 也包含 ab^{-1}.

证明 因为如果 H 包含 a，那末它就包含 $aa^{-1}=e$，所以 H 也包含 $ea^{-1}=a^{-1}$. 再如果 H 包含 a, b，它就包含 $a(b^{-1})^{-1}=ab$，因此定理得证.

譬如线性群 $GL(n, K)$ 中所有行列式为 1 的矩阵形成为子群，这是因为从 $|A|=1$, $|B|=1$，我们就有 $|A|\cdot|B^{-1}|=1$.

当群是加群时，a 的负元是 $-a$，因此定理 2 中所说的必要充分条件就是：假如 H 包含 a, b，那末 H 也包含 $a-b$.

特别当 H 是有穷集时，它成为子群的必要充分条件只是定理 1 中的条件 $1°$. 因为这时，我们可以把消去律来代替群定义的条件 $3°$, $4°$，但是消去律在 G 中是成立的，因此在 H 中也同样成立.

再我们来介绍对称群的重要子群——交代群.

我们首先来简化上节中排列的表示. 我们用(1 2 3 4)表示这样的排列, 它是把1换成2, 2换成3, 3换成4, 最后的4换成最前面的1, 其余的文字都不变动. 这种排列又常叫做**循环排列**. 由两个文字组成的循环排列, 叫做**对换**. 譬如(1 2)就是把1换成2, 2换成1, 其余的文字都不变动的对换. 为了方便, 我们更规定由一个文字组成的循环排列是恒等排列.

容易证明, 任意一个排列可以用没有公共文字的循环排列的乘积来表示, 譬如

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1\,3\,4)(2\,5),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1\,2\,3),$$

这时, 循环因子显然是可以相互交换的, 假如不计循环因子的顺序, 那末这种表示就是一意的. 又任意循环排列可以用对换的乘积来表示, 这种表示不是唯一的, 并且与因子的顺序有关. 譬如

$$\begin{aligned}(1\,2\,3\cdots n) &= (1\,2)(2\,3)\cdots(n-1\;n)\\ &= (1\,n)(1\;n-1)\cdots(1\,2),\end{aligned}$$

$$\begin{aligned}(2\,5) &= (1\,2)(1\,5)(1\,2) = (1\,5)(1\,2)(1\,5)\\ &= (4\,5)(3\,4)(2\,3)(3\,4)(4\,5).\end{aligned}$$

于是任意一个排列可以用对换的乘积来表示, 这表示不是唯一的, 但它有下面一个重要的不变性质.

定理3 假如一个排列用对换的乘积来表示, 那末对换因子的个数是偶数或奇数是一定的, 也就是说, 是偶数时永远是偶数, 是奇数时永远是奇数.

证明 假设 n 个文字 $a_1, \cdots, a_n$ 的函数

$$\begin{aligned}F &= \prod_{1\leq i<j\leq n}(a_i - a_j)\\ &= (a_{n-1} - a_n)\end{aligned}$$

$$\cdot(a_{n-2}-a_n)\cdot(a_{n-2}-a_{n-1})$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdot(a_1-a_n)\cdot(a_1-a_{n-1})\cdots(a_1-a_2),$$

我们把 F 写成

$$F=(a_k-a_l)\prod_{i\neq k,l}(a_i-a_k)(a_i-a_l)f,$$

这里 f 不包含 a_k 及 a_l. 现在 F 上施行对换 $(a_k\,a_l)$, 我们容易知道 f 及 $(a_i-a_k)(a_i-a_l)$ 都不变动, 但 (a_k-a_l) 变了符号, 所以 F 就换成为 $-F$. 这就是说, 在 F 上施行任一个对换, F 就变符号, 因此在 F 上假如继续施行偶数个对换, 结果仍然是 F, 假如继续施行奇数个对换, 结果就是 $-F$. 但是在 F 上施行一个排列的结果是一定的, 因此一个排列不能同时表为偶数个对换的乘积, 又表为奇数个对换的乘积, 所以定理成立.

一个排列, 它的对换因子的个数假如是偶数, 就叫做**偶排列**, 假如是奇数就叫做**奇排列**. 一个偶排列与一个奇排列的乘积是奇排列, 两个偶排列或两个奇排列的乘积都是偶排列. 恒等排列是偶排列[4].

因为两个偶排列的乘积仍然是偶排列, 所以在 n 个文字上的对称群 S_n 中所有偶排列形成一个子群, 叫做 n 个文字上的**交代群**, 用 A_n 来表示, 它是 S_n 中一个非常重要的子群. 再对称群 S_n 中偶排列个数与奇排列个数相等. 这是因为用 S_n 中某一奇排列乘其中所有偶排列就得到互异的奇排列, 因此 S_n 中偶排列不多于奇排列. 同样, S_n 中奇排列又不多于偶排列, 所以 S_n 中偶排列个数与奇排列个数相等. 因为 S_n 的元数是 $n!$, 所以 A_n 的元数是 $n!/2$.

譬如三个文字上的对称群

$$S_3=\{(1),(1\,2),(1\,3),(2\,3),(1\,2\,3),(1\,3\,2)\},$$

交代群

$$A_3=\{(1),(1\,2\,3),(1\,3\,2)\}.$$

最后来讨论循环群的子群，我们先介绍循环群.

假定 M 是群 G 的子集，当然它不一定成群，因为 M 中任意两元的积以及任意元的逆虽然都在 G 中，但不一定都在 M 中. 如果我们把这些积以及这些逆都添加于 M，那它就成为子群. 这子群包含 M，叫做由 **M 生成的群**，用(M)来表示，这时我们又说 M 是(M)的**生成元集**，M 中元又叫做(M)的**生成元**. 在 G 中，除 G 自身外，可能还有其他子群包含 M. 但是任意包含 M 的子群都包含(M)，所以(M)是 G 中所有包含 M 的子群的交集，因此(M)是 G 中包含 M 的最小子群. 当 M 自身是子群时，$(M)=M$.

假如 $M=\{a_1, a_2, \cdots, a_n\}$，并且其中任意两元 a_i, a_j 都能够交换，即 $a_ia_j=a_ja_i$，那末(M)是所有形状象

$$a_1^{m_1}a_2^{m_2}\cdots a_n^{m_n}$$

的元形成的子群，这里 m_i 是正、负整数或零.

特别，由一个元 a 生成的子群(a)是由元 a 的所有幂 a^n 形成的，这时

$$a^m\cdot a^n=a^{m+n},\ a^0=e,\ a^{-n}=(a^{-1})^n.$$

一个群如果是由其中一个元生成的就叫做**循环群**.

譬如 A_3 是元数是 3 的循环群，$(1\,2\,3)$，$(1\,3\,2)$都是它的生成元，即 $A_3=((1\,2\,3))=((1\,3\,2))$. 整数集 Z 对加法形成的加群是无穷循环群，1，-1 都是它的生成元，即 $Z=(1)=(-1)$.

循环群在群中是构造最简单的，并且也是最基本的. 下面我们来讨论循环群(a)的构造.

假定 a 的所有幂都互不相等，即当 $h\neq k$ 时，$a^h\neq a^k$，因此这时循环群(a)是由下面的元组成的：

$$\cdots,\ a^{-2},\ a^{-1},\ a^0,\ a^1,\ a^2,\ \cdots,$$

它是无穷群.

假定 a 的幂中有相等的，并且 $h>k$ 时，$a^h=a^k$，这时我们有

$$a^{h-k}=e, \quad h-k>0.$$

如果 n 是使 $a^n=e$ 成立的最小正整数，那末 $a^0, a^1, \cdots, a^{n-1}$ 彼此互异，这是因为假如

$$a^i=a^j, \quad 0\leqslant j<i<n,$$

那末

$$a^{i-j}=e, \quad 0<i-j<n.$$

这与 n 是最小正整数的假定矛盾.

再假如把任意整数 m 写成

$$m=qn+r, \quad 0\leqslant r<n,$$

那就有

$$a^m=a^{qn+r}=a^{qn}\cdot a^r=(a^n)^q\cdot a^r=ea^r=a^r,$$

所以 a 的任意幂都与 $a^0, a^1, \cdots, a^{n-1}$ 中某一个相等，因此这时循环群(a)只含有 n 个元

$$a^0, a^1, \cdots, a^{n-1},$$

它是有穷群，元数是 n.

假如 a 的任意两个乘幂都不相等，我们就说 a 的**阶**是无穷. 假如 a 的乘幂中有相等的，n 是使 $a^n=e$ 成立的最小正整数，我们就说 a 的**阶数**是 n.

譬如群的单位元的阶数是 1，A_3 的生成元$(1\ 2\ 3)$的阶数是 3. 再在整数集 Z 形成的加群中，任意非零的整数的阶都是无穷.

于是由上面的讨论，我们有

定理 4　一个循环群(a)，假如 a 的阶是无穷，那末它是无穷群：

$$(a)=\{\cdots, a^{-2}, a^{-1}, a^0, a^1, a^2, \cdots\},$$

假如 a 的阶数是 n，那末它是元数是 n 的有穷群：

$$(a)=\{a^0, a^1, \cdots, a^{n-1}\}, \quad a^n=a^0.$$

再我们容易得知，假如 a 的阶是无穷，那末当 $a^m=e$ 时，$m=$

0，因此 $a^r=a^s$ 的必要充分条件是 $r=s$．假如 a 的阶数是 n，那末，当 $a^m=e$ 时，$m\equiv 0(n)$，也就是说，m 是 n 的倍数，这是因为 m 可以写成 $m=qn+r$，$0\leqslant r<n$，于是

$$a^r=a^m\cdot a^{-qn}=a^m=e,$$

因为 n 是阶数，所以 $r=0$，即 $m=qn$，因此 $a^r=a^s$ 的必要充分条件是 $r\equiv s(n)$．

现在来讨论循环群的子群．

假设 G 是由元 a 生成的循环群，H 是 G 的子群，但不是单位元群，也就是说，H 不是只由单位元形成的，那末 H 中必含有幂 $m>0$ 的元 a^m．这是因为，假如 $m<0$，那末 a^m 的逆元 a^{-m} 也在 H 中，这时 $-m>0$．假设 a^m 是 H 中 a 的最小正幂，显然 H 包含 a^m 的任意乘幂．假如 a 是 H 中任意元，由 $s=tm+r$，$0\leqslant r<m$，我们得知

$$a^r=a^{s-tm}=a^s\cdot(a^m)^{-t}$$

也是 H 中元，但 m 是最小正整数，而 $0\leqslant r<m$，因此 $r=0$，于是

$$a^s=(a^m)^t,$$

这就是说，H 中任意元是 a^m 的乘幂，也就是说 H 只含 a^m 的任意乘幂，所以 H 是由 a^m 生成的循环群，即 $H=(a^m)$．因为 G 中任意元的 m 乘幂是 a^m 的乘幂，所以 H 又可以看成是由 G 中各元的 m 乘幂形成的子群．

假如 a 的阶是无穷，那末 a^m 的阶也是无穷，于是 H 是由下面无穷多个元形成的：

$$(a^m)^0=e,\quad a^{\pm m},\ a^{\pm 2m},\ \cdots,$$

所以这时它是无穷群．

假如 a 的阶数是 n，即 $a^n=e$．因为 m 是 H 中 a 的最小正幂，而 $a^n\in H$，所以 n 能够用 m 整除，命 $n=qm$，那末 a^m 的阶数是 q，于是 H 只包含下面 q 个元：

$$a^0,\ a^m,\ a^{2m},\ \cdots,\ a^{(q-1)m},$$

所以这时 H 是元数为 q 的有穷群. G 中元数是 q 的子群显然只是由 a^m 生成的,因此 G 只有唯一个 q 元子群.

由上面讨论的结果,我们有

定理 5 循环群 $G=(a)$ 的子群 H 还是循环群. 假如 H 不是单位元群, 那它就是由其中元 a 的最小正幂 a^m 生成的, 也就是说, H 是由 G 中所有各元的 m 幂形成的. 当 G 是无穷群时, H 也是无穷群. 当 G 的元数是 n 时, 这 n 是 m 的约数, 因此 H 的元数是 $q=\frac{n}{m}$, 并且 H 是 G 中唯一个 q 元子群.

于是, 无穷循环群有无穷个子群, n 元循环群的子群的个数等于 n 中互异正因数的个数.

群 G 中所有各元的 m 幂形成的子群, 我们用 G^m 表示, 于是由上定理, 我们得知循环群 G 的子群是 G^m, m 是正整数.

1956 年石兹(F. Szász)证明了它的逆, 即群 G, 如果它的子群都是 G^m, m 是正整数, 那末 G 是循环群. 因此群 G 是循环群的必要充分条件是它的子群都是 G^m(m 是正整数)的形状[5].

要注意的是, 循环群 (a) 中任意元 a^m 生成的群 (a^m) 当然都是 (a) 的子群, 但 a^m 不一定就是 (a^m) 中 a 的最小正幂. 当 (a) 是无穷群时, a^m 是 (a^m) 中 a 的最小正幂. 当 (a) 的元数是 n 时, 只有 $m|n$ 时, a^m 才是 (a^m) 中 a 的最小正幂. 譬如 $n=6$ 时, $(a^4)=(a^2)$, $(a^5)=(a)$.

循环群中两个子群相等与否, 我们有下面的定理.

定理 6 循环群 (a) 如果是无穷群, 那末它的子群 $(a^r)=(a^s)$ 的必要充分条件是 $r=\pm s$; 如果是元数为 n 的有穷群, 当 $s|n$ 时, $(a^r)=(a^s)$ 的必要充分条件是 r 与 n 的最大公因数 $(r,n)=s$.

证明 我们先证明定理的前半段. 当 $r=\pm s$ 时, 显然 $(a^r)=(a^s)$, 因此这时充分条件成立. 反过来, 假如 $(a^r)=(a^s)$, 那末 $a^r=$

$(a^s)^h=a^{sh}$,因此 $r=sh$. 同样 $s=rk$, 于是 $s=skh$, 即 $kh=1$, 但 h, k 都是整数,所以 $h=k=\pm1$, 于是 $r=\pm s$, 因此必要条件成立.

下面来证明定理的后半段. 假如 $(a^r)=(a^s)$, 因为 $a^r=(a^s)^h=a^{sh}$,所以 $r\equiv sh(n)$. 但由假设, $s|n$, 所以 $s|r$, 因此 s 是 r, n 的公因数. 同样我们又有 $s\equiv rk(n)$, 所以 r, n 的公因数都是 s 的因数,因此 s 是 r, n 的最大公因数, 即 $s=(r, n)$. 反过来, 假如 $s=(r, n)$, $a^{s'}$ 是 (a^r) 中 a 的最小正幂, 由定理 5, $(a^r)=(a^{s'})$, 并且 $s'|n$, 于是由上面已证得的必要条件, $s'=(r, n)$, 因此 $s=s'$, 即 $(a^r)=(a^{s'})=(a^s)$, 所以定理成立.

特别,当 $s=1$ 时,我们即得: 循环群 (a), 如果是无穷群, 那末只有两个元 a, a^{-1} 可做它的生成元, 即 $(a)=(a^{-1})$. 如果是元数是 n 的有穷群, 因为小于 n 且与 n 互质的正整数有 $\varphi(n)$ (叫做欧拉(L. Euler, 1707～1783)函数)个,所以有 $\varphi(n)$ 个元 a^r 可做它的生成元, 即 $(a)=(a^r)$, 这里 $(r, n)=1$, $r<n$.

譬如, n 次单位根也就是 n 次多项式 x^n-1 的零点

$$\xi_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n},\quad h=1, \cdots, n$$

形成 n 元循环群, 它的生成元是 ξ_r, 这里 $(r, n)=1$. 因此元数是任意自然数的循环群是存在的.

一个群究竟有多少个子群以及子群的构造如何, 这是群论中主要问题之一, 在一般情况下, 这问题还没有得到解决. 由定理 4 及定理 5, 我们得知对于循环群来说这问题算是解决了的. 密勒尔(G. A. Miller)曾由子群的个数及性质来讨论群的构造,得到了不少的好结果[6],这里当然都不能谈了.

习 题 2.2

1. 试证下列各式:

$$(1\,2)(3\,4)(1\,5)(2\,3)(4\,5)=(1\,5\,3)(2\,4),$$

$$(1\,i\,j)=(1\,2\,j)^2(1\,2\,i)(1\,2\,j),\ (a\,c)(b\,d)=(a\,b\,d)(a\,c\,d).$$

2. 试求循环加群 $Z=(100)$ 的所有子群.

3. 假定元 a 的阶数是 n，而 $a^m=e$. 试证 n 是 m 的因数.

4. 一个循环排列，它所含文字的个数如果是偶数，就是奇排列，如果是奇数，就是偶排列，怎样证明？

5. 假定 $a,\ b$ 是群中元，$ab=ba$，元 a 的阶数是 m，元 b 的阶数是 n，那末它们的乘积 ab 的阶数是 $m,\ n$ 的最小公倍数 q 的约数，并且群中含有阶数是 q 的元，当 $m,\ n$ 互质时，ab 的阶数是 mn.

6. 假如可换群 G 中元的最大阶数是 m，试证 G 中任意元的阶数都是 m 的因数.

7. 写出 4 个文字上的交代群 A_4 的群表.

8. 证明 S_n 可以用 $n-1$ 个对换 $(1\,2),\ (1\,3),\ \cdots,\ (1\,n)\ (n>1)$ 生成.

9. 证明 A_n 可以用 $n-2$ 个 3 项循环排列 $(1\,2\,3),\ (1\,2\,4),\ \cdots,\ (1\,2\,n)$ 生成.

10. 假如 $\tau,\ \sigma$ 是两个排列，如果把 τ 写成没有公共元的循环排列的乘积，并且循环排列中的文字用 σ 里面所变换的文字来代替，那末所得的排列就是 $\sigma\tau\sigma^{-1}$. 譬如 $\tau=(3\,1\,4)(2\,5)(6\,7)$，$\sigma=(1\,2\,3)(5\,6\,7)$，那末 $\sigma\tau\sigma^{-1}=(1\,2\,4)(3\,6)(7\,5)$. 这是为什么？

§2.3 正规子群

在 §1.2 中我们曾经把整数集 Z 用子群 (n) 来分类，现在我们把它推广，来讨论一般群用它的子群来分类.

我们先介绍子集乘积的概念.

假设 $H,\ K$ 是群 G 的两个子集，h 是 H 中任意元，k 是 K 中任意元，那末所有元 hk 的集，叫做 H 与 K 的乘积，或简称 $H,\ K$ 的积，用记号 HK 来表示. 譬如 $H=\{(1),\ (1\,2),\ (1\,2\,3)\}$，$K=\{(1\,2\,3),\ (1\,3\,2)\}$，那末

$$HK=\{(1),\ (1\,3),\ (2\,3),\ (1\,3\,2)\}.$$

关于三个子集的乘积,我们有

$$H(KL)=(HK)L.$$

这就是说,群中子集的乘积是满足结合律的。

当 H 是子群时,我们又有

$$HH=H.$$

要注意,它的逆不成立,即当 $HH=H$ 时, H 不一定成群.

假定 H, K 都是 G 的子群, H, K 的乘积 HK 一般不一定成群. 现在我们要问在什么条件下, HK 也成为群?

假如 HK 成群, h, k 分别是 H, K 中任意元, 因为 KH 中元 kh 是 HK 中元 $h^{-1}k^{-1}$ 的逆, 所以 $kh\in HK$, 因此 $KH\subseteq HK$. 又因为 $(hk)^{-1}\in HK$, 命 $(hk)^{-1}=h'k'$, 于是 $hk=k'^{-1}h'^{-1}\in KH$, 所以 $HK\subseteq KH$. 因此 $HK=KH$, 也就是说, 假如 HK 成群,那末 H 与 K 能够交换.

反过来,假如 $HK=KH$,也就是说,H 与 K 能够交换,那末 HK 中任意元 hk 的逆元 $k^{-1}h^{-1}$ 在 HK 中. 又因为

$$HKHK=HHKK=HK,$$

所以 HK 中任意两元的乘积仍然在 HK 中,于是 HK 成群. 因此我们有下面的

定理 1 群 G 的子群 H, K 的乘积 HK 成群的必要充分条件是 H 与 K 能够交换.

要注意的是,这里说的 H 与 K 能够交换, $HK=KH$, 是表示 $HK\subseteq KH$,并且 $KH\subseteq HK$,因此对于 H, K 中任意元 h,k, 我们不一定就能有 $hk=kh$, 一般只能有 $hk=k'h'$, $kh=h''k''$, 这里 h', h''; k', k'' 分别是 H, K 中元. 当 G 是可换时, 显然 $HK=KH$. 所以可换群的任意两个子群的乘积仍然是一个子群.

由 §2.2, 我们知道 HK 包含在由 H, K 生成的群中, 当 HK 成群时,由 H, K 生成的群就是 HK,即 $(H, K)=HK$,也

就是说，HK 是 G 中包含 H, K 的最小子群。

假如 G 是加群，只要 H, K 是子群，当然 HK 也是子群，这时仍然把 HK 写成 (H, K)，叫做 H, K 的**和**，我们不用 $H+K$ 来表示，因为后面（§5.4）要用它来表示直和。

特别当 H 只包含一个元 h 时，H 与 K 的乘积 HK 就简单地写成 hK.

定义 1 假如 H 是 G 的子群，a 是 G 中任意元，那末集合 $aH(Ha)$，叫做 G 中 H 的**左（右）陪集**.

譬如 $G=S_3$, $H=\{(1), (1\,2)\}$，那末 H 的左陪集

$$(1\,3)H=\{(1\,3), (1\,2)\}, \quad (2\,3)H=\{(1\,2\,3), (1\,3\,2)\};$$

H 的右陪集

$$H(1\,3)=\{(1\,3), (1\,3\,2)\}, \quad H(2\,3)=\{(2\,3), (1\,2\,3)\}.$$

因此一个群的子群的左陪集不一定与它的右陪集一致. 当群是可换群时，陪集就无所谓左、右的了.

假如 a 在 H 中，那末 $aH=H$，这就是说，H 自身也是一个左陪集. 假如 $b\in aH$，那末 $aH=bH$，这就是说，左陪集 aH 由其中任一元一意确定. 假如 a, b 在 H 的同一左陪集中，那末 $b=ah$，因此 $a^{-1}b=h\in H$. 反过来，假如 $a^{-1}b\in H$，那末 $b=ah$，因此 a, b 在 H 的同一左陪集中. 于是 a, b 在 H 的同一左陪集的必要充分条件是 $a^{-1}b\in H$.

假如 aH 成群，那末 $a\in H$，因此 $aH=H$，这就是说，H 的陪集中只有 H 成群，其余都不成群.

假如把 aH 的元 ah 与 bH 的元 bh 相对应，我们就得到 aH 射到 bH 上的一对一的映射，因此两个左陪集 aH, bH 的浓度相等.

现在我们来讨论群 G 用它的子群 H 的陪集来分类.

因为 G 中任意元 a 必出现在 H 的左陪集 aH 中. 假如左陪

集 aH, bH 有公共元 $ah=bh'$,那末 $a^{-1}b=hh'^{-1}\in H$, 因此 $aH=bH$. 就是说, G 中 H 的任意两个左陪集或者重合或者没有公共元. 于是 G 可以分解为若干个互异的左陪集 a_iH, $i=1, 2, \cdots$, 即

$$G=a_1H\cup a_2H\cup\cdots.$$

同样,我们可以把 G 分解为若干个互异的右陪集 Hb_i, $i=1, 2, \cdots$, 即

$$G=Hb_1\cup Hb_2\cup\cdots.$$

用同一个子群把群分解为左陪集与分解为右陪集,其结果一般是不一致的. 譬如交代群 A_4 对于克莱茵(F. Klein, 1849~1925)四元群

$$B_4=\{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

的左陪集分解与右陪集分解分别为

$$A_4=B_4\cup(2\,3\,4)B_4\cup(2\,4\,3)B_4=B_4\cup B_4(2\,3\,4)\cup B_4(2\,4\,3).$$

又对称群 S_3 对于 $H=\{(1), (1\,2)\}$的两种分解为

$$S_3=H\cup(1\,3)H\cup(2\,3)H=H\cup H(1\,3)\cup H(2\,3).$$

但 $(2\,3\,4)B_4=B_4(2\,3\,4)$, $(2\,4\,3)B_4=B_4(2\,4\,3)$, 而 $(1\,3)H\neq H(1\,3)$, $(2\,3)H\neq H(2\,3)$. 所以 A_4 对于 B_4 的两种分解是一致的,而 S_3 对于 H 的两种分解是不一致的. 下面是一个重要关系.

定理 2 假设 H 是群 G 的子群,并且

$$G=a_1H\cup a_2H\cup\cdots\cup a_nH\cup\cdots,$$

那末

$$G=Ha_1^{-1}\cup Ha_2^{-1}\cup\cdots\cup Ha_n^{-1}\cup\cdots.$$

证明 我们只要证明 G 中任意元 g 在某个右陪集 Ha_i^{-1} 中,并且任意两个右陪集 Ha_i^{-1}, Ha_j^{-1} 都不相等就行了.

首先因为 $g\in G$, 所以 $g^{-1}\in G$. 因此 g^{-1} 在某一左陪集 a_iH 中,即 $g^{-1}=a_ih$,于是 $g=h^{-1}a_i^{-1}\in Ha_i^{-1}$.

再如果 $Ha_i^{-1}=Ha_j^{-1}$, 那末 $a_i^{-1}a_j\in H$, 因此 $a_iH=a_jH$, 这与

假设不合，所以 Ha_i^{-1}, Ha_j^{-1} 是相异的右陪集，因此定理得证.

因为集合 $\{a_1, a_2, \cdots, a_n, \cdots\}$ 与集合 $\{a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1}, \cdots\}$ 显然有相等的浓度，所以 G 中 H 的相异左陪集的个数（即浓度），与相异右陪集的个数一致. 这样我们有

定义 2 群 G 中子群 H 的相异左（右）陪集的个数，叫做 H 在 G 的**指标**，用记号 $(G:H)$ 表示.

因为对左陪集能够成立的性质，对右陪集来说也能够同样证明，所以后面我们讨论陪集时，只就左陪集来讨论.

指标可以是有穷也可以是无穷. 譬如从 §1.2, $(Z:(n))=n$, 又 $(A_4:B_4)=3$, $(S_3:H)=3$. 再假如 G 是所有有理数对加法形成的加群，H 是所有偶数形成的子群，那末 $(G:H)$ 是无穷，这是因为，对于任一奇数 a，显然

$$a, \frac{1}{2}a, \cdots, \frac{1}{2^n}a, \cdots$$

分别在 H 的不同陪集中.

假如群 G 的元数是 n，它的子群 H 的元数是 m，如果 H 在 G 的指标是 j，那末

$$n=jm,$$

这是因为 G 有 j 个互异的左陪集，并且每个左陪集又都有 m 个元. 于是我们得下面的拉格朗日 (J. Lagrange, 1736～1813) 定理.

定理 3 有穷群的子群的元数是这群的元数的因数.

由这定理，我们容易得知当 p 是质数时，p 元群没有异于单位元群的真子群. p^n 元循环群只有 $n-1$ 个真子群.

1939 年密勒尔 (G. A. Miller) 曾证明，含 11 个真子群的群只有元数是 p^{12} 的循环群[7].

定理 3 是有穷群的一个重要性质，在很多地方我们将要引用

它.特别因为由一个元生成的循环群的元数就是这元的阶数,因此一个元的阶数是这群的元数的因数. 于是对于 n 元群中任意元 a,我们有

$$a^n=e.$$

拉格朗日定理的逆对于循环群显然成立,就是对于可换群也是成立的(§5.5),但一般不成立. 这就是说,假定 G 的元数是 n,如果 $m|n$,那末 G 不一定有 m 元子群. 譬如交代群 A_4 是 12 元群,但它没有 6 元子群. 假如 m 再满足某些条件,这逆定理还是能成立的,下面是著名的西洛(L. Sylow, 1832～1918)定理.

定理 4 假定有穷群 G 的元数是 n,p 是 n 的质因数,那末 G 有 p^a 元子群,叫做 G 属于 p 的西洛子群,或简称 p **西洛子群**,这里 $n=p^aq$,$p\nmid q$.

譬如 A_4 的元数是 $12=2^2\cdot 3$,那末 B_4 是它的 2 西洛子群,(2 3 4)生成的 3 元循环群是它的 3 西洛子群.

在这里我们只把定理提出,至于证明,因为需要另外的性质,所以把它放在 §5.6 中后半段.

下面我们引用陪集介绍正规子群的定义并给出一些基本性质,在后两节及第五章中我们将看到在另一些基本性质中,正规子群是非常重要的子群,在讨论群时,几乎处处都需要它.

一般 H 的左陪集不一定又是右陪集. 假如 H 的一个左陪集同时又是 H 的右陪集,那末对于这陪集中任意元 a,我们有 $aH=Ha$,也就是说 a 与 H 能够交换.

定义 3 假如群 G 中子群 H 的任意左陪集同时又是 H 的右陪集,也就是说,H 能够与 G 中任意元 a 交换,即

$$aH=Ha, \tag{1}$$

那末 H 叫做 G 的**正规子群**.

譬如对称群 S_3 的子群{(1), (1 2 3), (1 3 2)}是它的正规子

群，而子群$\{(1),(1\,2)\}$，$\{(1),(1\,3)\}$，$\{(1),(2\,3)\}$都不是它的正规子群. 群 G 自身及单位元群显然都是 G 的正规子群.

上面(1)式可以改写成不等式

$$aHa^{-1}\subseteq H,\quad a\in G.$$

这是因为上面不等式对于 G 中任意元都成立，当然对于 a^{-1} 也同样成立，因此 $a^{-1}Ha\subseteq H$，即 $H\subseteq aHa^{-1}$，所以 $aHa^{-1}=H$，也就是 $aH=Ha$，这就是说，G 的子群 H，如果包含元 h，它也包含所有的 aha^{-1}，$a\in G$，那末 H 就是 G 的正规子群.

假定 H 是线性群 $GL(n, K)$ 中所有行列式是 1 的矩阵形成的子群，a，h 分别是 $GL(n, K)$，H 中任意元，我们容易得知 aha^{-1} 的行列式是 1，所以 $aHa^{-1}\subseteq H$，因此 H 是 $GL(n, K)$ 的正规子群.

我们知道奇排列的逆是奇排列，偶排列的逆是偶排列，因此对于对称群 S_n 中任意排列 s，显然 sA_ns^{-1} 的排列都是偶排列，即 $sA_ns^{-1}\subseteq A_n$，所以 A_n 是 S_n 的正规子群.

我们知道可换群的子群都是正规子群，但它的逆不成立，也就是说，有这样的非可换群存在，它的任意子群都是正规子群，这类非可换群叫做汉弥尔顿(W. R. Hamilton, 1805～1865)群[9].

我们容易证明，群 G 中所有与 G 中任意元能够交换的元形成一个正规子群，这是 G 的一个重要正规子群，叫做 G 的**中心**. 假如 G 是可换，那末 G 的中心就是它自身. 当 G 的中心是单位元群时，有时又说 G **没有中心**. 譬如由$(1\,2)$，$(1\,4)(2\,3)$生成的群$((1\,2),(1\,4)(2\,3))$的中心是$\{(1),(1\,2)(3\,4)\}$，S_3 的中心是单位元群，因此 S_3 没有中心.

我们知道子群这个关系是适合传递律的，但正规子群就不是这样，这就是说，假如 H 是 K 的正规子群，K 是 G 的正规子群，那末 H 不一定就是 G 的正规子群. 譬如克莱茵四元群 B_4 是对

称群 S_4 的正规子群，因为 B_4 是可换群，所以{(1), (1 2)(3 4)}是 B_4 的正规子群，但它不是 S_4 的正规子群.

显然，在同一个群中两个正规子群的乘积是一个正规子群；一个子群与一个正规子群的乘积是一个子群.

再由定义得知，假如 G 的子群 H 是正规子群，那末 G 中任意元与 H 能够交换. 假如 H 不是正规子群，那末 G 中有与 H 不能够交换的元. G 中所有与 H 能够交换的元形成子群 K，叫做 G 中 H 的**正规化群**. 显然 $H\subseteq K\subseteq G$，并且 H 是 K 的正规子群. 譬如交代群 A_4 的子群{(1), (2 3 4), (2 4 3)}的正规化群就是它自身.

一个群至少有两个正规子群，一个是它自身，一个是单位元群. 只有这两个正规子群的群，就叫做**单纯群**，或简称**单群**. 显然，单位元群是单群，元数是质数的群也是单群. 再由于拉格朗日定理的逆对于可换群成立，我们容易得知可换群只在元数是 1 或者是质数时，才是单群.

至于非可换群，元数不大于 1000 的只有元数是

$$60,\ 168,\ 360,\ 504,\ 660$$

的五个是单群. 狄克生 (L. E. Dickson, 1874～1954) 曾揭示元数不大于百万的单群只有 53 个[10]. 这 53 个单群，它们的元数都是偶数. 是不是非可换单群的元数都是偶数，这是群论中长期没有得到证明的问题，1963 年已由怀特 (W. Feit) 及汤卜生(J. G. Thompson) 予以证实[11].

下面是正规子群的一个重要性质.

假如 H 是 G 的正规子群，那末 G 中元 a 所在的左陪集 aH 与元 b 所在的左陪集 bH 的乘积

$$aH\cdot bH=aHb\cdot H=ab\cdot HH=abH.$$

如果我们把 a 所在的左陪集 aH 用 $\bar{a}$ 表示，那就有

$$\bar{a}\cdot\bar{b}=\overline{ab}.$$

因此 G 中所有 H 的左陪集形成一个乘集. 再我们容易知道, H 自身是这乘集的单位元, $\overline{a^{-1}}$ 是 $\bar{a}$ 的逆元, 即 $\bar{a}^{-1}=\overline{a^{-1}}$. 又因为 G 中元 a, b, c 满足结合律, 所以左陪集 $\bar{a}$, $\bar{b}$, $\bar{c}$ 也满足结合律. 因此把 H 的左陪集看成为元素时, 所有这些左陪集形成为群, 叫做 G 关于 H 的**商群**, 用 G/H 表示. 它的元数显然是 H 在 G 的指标.

当 G 是加群时, G 中 H 的陪集又叫做 H 的**同余类**, 因此 G 关于 H 的商群又叫做**同余群**, 因为它是加群, 所以又常常叫做**同余加群**, 有时又叫做**差群**, 用 $G-H$ 表示. 假如 G 是加群, H 是它的子群, 如果 G 中元 a, b 同在 H 的一个同余类, 那末它们的差 $a-b\in H$, 我们用同余式

$$a\equiv b\,(\mathrm{mod}\,H) \text{ 或 } a\equiv b\,(H)$$

表示, 这时 a, b 又叫做关于 H 是**同余**. 当 $a\equiv 0(H)$ 时, a 属于 0 所在的同余类, 因此 $a\in H$. 假如 $H=(h)$, 我们又常常把 $a\equiv b(H)$ 写成 $a\equiv b(h)$, 因此 §1.2 所用的记号就是这里的特例.

譬如整数集 Z 关于 (n) 的同余加群 $Z-(n)=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$, 它的元数是 n, 这时它的结合法是 $\bar{a}+\bar{b}=\overline{a+b}$, 也就是当 $a+b\equiv c(n)$ 时 $\bar{a}+\bar{b}=\bar{c}$.

我们知道, 可换群的商群当然还是可换群, 但它的逆并不成立, 也就是说, 有时非可换群的商群也是可换群. 最后我们介绍一个具有这性质的重要正规子群来结束本节.

假定 a, b 是群 G 中任意元, 如果 $ab=ba$, 那末 $a^{-1}b^{-1}ab=e$. 如果 $ab\neq ba$, 命 $a^{-1}b^{-1}ab=c$, 那末 $ab=ba\cdot c$, 这就是说 ba 用 c 右乘后就变成为 ab 了, 因此我们叫 c 做 a, b 的**换位子**. 当 G 是可换群时, 只有单位元是它的换位子. 反过来, 一个群的换位子如果只是单位元, 显然这群是可换群. 一个群的两个换位子的乘积一般不再是这群的换位子[12]. 因此一个群的所有换位子不一定形成为

群．我们叫 G 中所有换位子生成的群做 G 的**换位子群**，用 $D(G)$ 或 G' 来表示．

假定 G' 是 G 的换位子群，a, g 分别是 G, G' 中任意元，因为 g 也是 G 中元，由 $aga^{-1}g^{-1}\in G'$，我们有

$$aga^{-1}g^{-1}\cdot g=aga^{-1}\in G',$$

因此 $aG'a^{-1}\subseteq G'$，所以 G' 是 G 的正规子群．再由 $a^{-1}b^{-1}ab=g$，我们有 $ab=bag$，于是 $\overline{ab}=\overline{ba}$，即 $\bar{a}\bar{b}=\bar{b}\bar{a}$，因此商群 G/G' 是可换群．

又假如 G/H 是可换群，由 $\bar{a}\bar{b}=\bar{b}\bar{a}$，我们就有 $ab=bah$，$h\in H$，因此 $a^{-1}b^{-1}ab\in H$，这就是说 H 包含 G'．反过来，假如 H 是包含 G' 的正规子群，那末 G/H 是可换群，于是我们有

定理 5 群 G 的换位子群 G' 是 G 的正规子群，并且商群 G/G' 是可换群．G/H 是可换群的必要充分条件是 H 包含 G 的换位子群 G'．

我们容易知道 S_n/A_n 是可换群，所以 $D(S_n)\subseteq A_n$，再由 §2.2 习题 9，A_n 是所有 3 项循环排列 $(1\,2\,i)$ 生成的群，但任意 3 项排列

$$(1\,2\,i)=(2\,1)^{-1}(i\,1)^{-1}(2\,1)\,(i\,1),$$

即 $(1\,2\,i)$ 是 S_n 的换位子，因此 $A_n\subseteq D(S_n)$．所以 $D(S_n)=A_n$．又当 $n\geqslant 5$ 时，

$$\begin{aligned}(1\,a\,2)^{-1}(1\,b\,i)^{-1}(1\,a\,2)\,(1\,b\,i)&=(1\,2\,a)\,(1\,i\,b)\,(1\,a\,2)\,(1\,b\,i)\\&=(12i),\end{aligned}$$

即 $(1\,2\,i)$ 是 A_n 的换位子，因此 $D(A_n)=A_n$，于是我们有

定理 6 对称群 S_n 的换位子群是交代群 A_n．当 $n\geqslant 5$ 时，A_n 的换位子群是 A_n 自身．

习 题 2.3

1. 试证元数是质数的群是循环群．

2．试证指标是2的子群是正规子群．

3．假定 H 是 G 的子群，K 是 H 的子群，求证

$$(G:K)=(G:H)(H:K).$$

4．假定 G 是循环群，H 是指标为 m 的子群，那末 G/H 是元数为 m 的循环群．因此任意循环群 G 的子群 H 在 G 的指标 $(G:H)$ 是有穷的．

5．群 G 中子群 H 是正规子群的必要充分条件是：H 的任意两个左陪集的乘积仍然是 H 的一个左陪集，如何证明？

6．试求 S_4 的 2 西洛子群

$$B_8=\{(1),\ (1\,2),\ (3\,4),\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3),\ (1\,4\,2\,3),\ (1\,3\,2\,4)\}$$

的正规子群及它的中心．

7．具有关系　$i^2=j^2=k^2=-1,\ (-1)^2=1,$

$$ij=k=-ji,\ jk=i=-kj,\ ki=j=-ik$$

的数 i, j, k 是基本四元数（§3.2），因此，由 $\pm i,\ \pm j,\ \pm k,\ \pm 1$ 等 8 个数形成的 8 元群，叫做**四元数群**．试证四元数群的 2 元子群只有 (-1) 一个，4 元子群有 (i)，(j)，(k) 三个，并且它们都是正规子群．于是四元群是汉弥尔顿群．

8．试求交代群 A_4 的子群，并指出何者是正规子群．

9．试证交代群 A_3 的换位子群是单位元群，A_4 的换位子群是克莱茵四元群 B_4．

10．试证对称群 S_n，$n\geqslant 3$ 的中心是单位元群．

11．试证对称群 S_4 的正规子群除自身及单位元群外，只有交代群 A_4 及克莱茵四元群 B_4．

12．假如已知 $n>4$ 时交代群 A_n 是单群，试证 $n\neq 4$ 时，对称群 S_n 除自身及单位元群外，只有 A_n 是它的唯一正规子群．

§2.4　同　　构

映射这个概念，对于代数系必须与结合法或代数运算发生联系，才能成为有力工具．因此在讨论代数系时，我们需要的是与结合法有联系的映射．显然，两元的乘积的象等于这两元的象的乘

积是一个重要关系，此后两节就是讨论具有这种联系的重要映射.

定义 假设 M, M' 是两个乘集，也就是说，M, M' 是两个各具有一个闭合的结合法（写成乘法）的代数系，σ 是 M 射到 M' 上的可逆映射，并且任意两元的乘积的象是这两元的象的乘积，即对于 M 中任意两元 a, b,

$$\sigma(a\cdot b)=\sigma(a)\cdot\sigma(b),$$

也就是说，当 $a\to\sigma(a)$, $b\to\sigma(b)$ 时，$ab\to\sigma(a)\sigma(b)$，那末这映射 σ 就叫做 M 射到 M' 上的**同构**. 我们又叫 M 与 M' **同构**，用 $M\cong M'$ 表示.

譬如结合法都是乘法的两个群

$$G=\{1,\ i,\ -1,\ -i\},\quad G'=\{\sigma_0,\ \sigma_{90},\ \sigma_{180},\ \sigma_{270}\},$$

这里 σ_i 是绕一固定直线旋转 i^0 的空间旋转. 如果命

$$1\to\sigma_0,\ i\to\sigma_{90},\ -1\to\sigma_{180},\ -i\to\sigma_{270},$$

显然这映射是 G 射到 G' 上的同构，因此 $G\cong G'$.

再假如 M 是所有实数形成的乘集，它的结合法是普通加法，M' 是所有正实数形成的乘集，它的结合法是普通乘法，那末

$$a\to\sigma(a)=10^a$$

就是 M 射到 M' 上的同构. 这是因为，对于 M 中任意元 a，它在 M' 中的象是 10^a. 反过来，对于 M' 中任意元 b，它在 M 中的象源是 $\log_{10}b$，并且当 $10^{a_i}=10^{a_j}$ 时，$a_i=a_j$，所以 σ 是 M 射到 M' 上的可逆映射. 再因为 $\sigma(a_i)=10^{a_i}$, $\sigma(a_j)=10^{a_j}$，所以

$$\sigma(a_i+a_j)=10^{a_i+a_j}=10^{a_i}\cdot10^{a_j}=\sigma(a_i)\cdot\sigma(a_j).$$

因此 $M\cong M'$.

又由 §2.2 定理 4，我们容易验证，循环群 (a) 假如是无穷群，那末它与整数集 Z 形成的加群同构，这时 $a^i\to i$ 是它们的同构映射. 假如是元数为 n 的有穷群，那末它与加群 Z 关于 (n) 的同余

加群 $Z-(n)$ 同构，这时它们的同构映射是 $a^i\to\bar{i}$. 因此任意两个无穷循环群都同构，有穷循环群只要它们的元数相等也都同构.

由§2.1 习题 9, 我们得知，群 G 的所有变换 $\sigma_a(g)=ag$, $a\in G$, 形成群 G', 假如命 a 与 σ_a 对应，即 $a\to\sigma_a$, 那末这对应显然是 G 射到 G' 上的可逆映射；又因为 $\sigma_{ab}=\sigma_a\sigma_b$, 所以它又是 G 射到 G' 上的同构，因此 $G\cong G'$. 于是我们有下面的**卡莱定理**.

定理 1　任意群与它的变换群的子群同构.

当 G 是有穷群时，命 $G=\{a_1, a_2, \cdots, a_n\}$, 那末变换 σ_a 就是排列

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ aa_1 & aa_2 & \cdots & aa_n \end{pmatrix},$$

因此 G 就与对称群 S_n 的子群同构，也就是说，任意有穷群与对称群的子群同构.

1942 年汤璪真(1898～1951)发表了这样一个定理，假定 G 是群，u 是其中任意元，如果对于 G 中任意元 a, b, 规定另一个结合法$\circ$, $a\circ b=au^{-1}b$, 那末 G 中元对于这种结合法形成与 G 同构的群，u 是它的单位元，$a\to au^{-1}$ 是它们的同构映射[13]. 读者试根据定义加以验证.

要注意的是两个乘集 M, M' 假如同构，我们最少有一个自 M 射到 M' 上的同构映射，但是这种映射一般不只一个，譬如在前面的同构映射 $a\to10^a$ 中，如果把 10 换成任意正整数 b, 显然 $a\to b^a$ 也是它们的同构映射.

假如两个乘集 M, M' 同构，$M\cong M'$, 那末 M, M' 的乘法表，除元素的记号及行，列的顺序外，在构造上完全是一样的. 因此，假如在 M 的元素间有一个用结合法表示的性质，那末在 M' 的元素间也有一个完全与它类似的性质；反过来也成立. 因为我们讨论 M, M' 是讨论 M, M' 中元素间运算的性质，所以两个同构的

群在本质上就没有区别. 也就是说，同构的群只用群的性质就无法区别它们，于是同构的群就可以看成是相同的群，因此一个群如果能够使它与已经研究清楚了的群同构，那末这个群也就是研究清楚了的. 但同构的群与相同的群是有区别的，譬如加群 Z 与所有偶数形成的群同构，但后者是前者的子群.

因为可逆映射是等价关系，所以同构这个关系也是等价关系.

在定义中，如果 $M'=M$，那末 σ 就叫做 M 的自同构，因此 M 的自同构就是 M 射到自己上的可逆映射. 恒等映射显然是自同构. 再假如 G 是可换群，那末把 a 变成它的逆元 a^{-1} 的映射是它的自同构.

我们知道，一个集的所有变换形成一个变换群，自同构是变换，是否一个乘集的所有自同构也能够形成为群？假如它们成为群，当然这个群是变换群的子群.

定理 2 乘集 M 的所有自同构形成为群，叫做 M 的自同构群.

证明 假如 σ, τ 是 M 的自同构，因为

$$\sigma\tau(a)=\sigma(\tau(a)),$$

所以

$$\begin{aligned}\sigma\tau(a_i a_j)&=\sigma(\tau(a_i a_j))=\sigma(\tau(a_i)\tau(a_j))\\&=\sigma\tau(a_i)\sigma\tau(a_j),\end{aligned}$$

因此 σ, τ 的积 $\sigma\tau$ 是 M 的自同构.

再因为

$$\sigma^{-1}\sigma(a)=a,\quad \sigma\sigma^{-1}(a)=a,$$

所以

$$\begin{aligned}\sigma^{-1}(a_i a_j)&=\sigma^{-1}(\sigma\sigma^{-1}(a_i)\sigma\sigma^{-1}(a_j))\\&=\sigma^{-1}(\sigma(\sigma^{-1}(a_i)\sigma^{-1}(a_j)))\end{aligned}$$

$$=\sigma^{-1}(a_i)\sigma^{-1}(a_j).$$

于是σ的逆σ^{-1}也是M的自同构，因此M的所有自同构成群，所以定理成立.

我们容易得知，群的自同构是把生成元仍然变为生成元，因此循环群(a)，假如是无穷群，因为它只有a, a^{-1}两个生成元，所以它的自同构也只有两个. 一个是把a仍然变为a，即恒等同构；另一个是把a变为a^{-1}，因此这时(a)的自同构群是2元循环群. 假如(a)是n元循环群，因为它有$\varphi(n)$个生成元a^r，这里$(r,n)=1$，$r<n$，所以它有$\varphi(n)$个自同构$\sigma_r(a)=a^r$，因此这时(a)的自同构群与$Z-(n)$中所有$\bar{r}$，$(r,n)=1$，对于乘法形成的群同构.

当$n\neq6$时，n个文字上的对称群S_n的自同构群与S_n自身同构，这结果早在1895年已由赫尔特尔(O. Hölder, 1859～1931)证明；1940年色格尔(Iruing E. Segal)给出一个简单证明，读者如欲知其详，请参看文献[14].

不同构的群它们的自同构群可能同构. 譬如无穷循环群与3元循环群的自同构群都是2元群. 因此群自身的性质不能转移到它的自同构群上.

下面我们来介绍群的一种重要的自同构.

假定a是群G的一个元. 那末映射σ:

$$g\to g'=aga^{-1},\quad g\in G,$$

是G的自同构. 这是因为，元g的象源是$a^{-1}ga$，如果

$$aga^{-1}=aha^{-1},$$

那末$g=h$，所以σ是G射到自己上的可逆映射，再从

$$g'=aga^{-1},\quad h'=aha^{-1},$$

我们就有

$$(gh)'=agha^{-1}=aga^{-1}\cdot aha^{-1}=g'h',$$

因此σ是G的自同构.

由一个元 a 决定的自同构 $g\to aga^{-1}$，叫做**内(自)同构**，其他的自同构，叫做**外(自)同构**．元 aga^{-1} 叫做 g 用 a 得到的**变形**，g 叫做与 aga^{-1} **共轭**．

假如 $\sigma(g)=aga^{-1}$，那末 $\sigma^{-1}(g)=a^{-1}ga$．再假如 $\tau(g)=bgb^{-1}$，那末 $\sigma\tau(g)=(ab)g(ab)^{-1}$，这就是说，内同构的逆是内同构，两个内同构的乘积又是内同构，因此群 G 的所有内同构形成一个群，叫做 G 的**内同构群**．

定理 3 一个群的内同构群是它的自同构群的正规子群．

证明 假定 σ 是群 G 的任意自同构，τ 是 G 的任意内同构，$\sigma(g)=h, \tau(g)=aga^{-1}$．于是

$$\begin{aligned}\sigma\tau\sigma^{-1}(h)&=\sigma\tau(g)=\sigma(aga^{-1})=\sigma(a)h\sigma(a^{-1})\\&=\sigma(a)h(\sigma(a))^{-1},\end{aligned}$$

因此 $\sigma\tau\sigma^{-1}$ 是内同构，所以定理成立．

1895 年赫尔特尔又证明了这样一个定理，在对称群中，有外同构的只有一个 S_6[15]．因此当 $n\neq 6$ 时，对称群 S_n 的自同构群都是内同构群．

假定 σ 是群 G 的自同构，H 是 G 的子群，如果 $\sigma(H)\subseteq H$，我们就说 H 对 σ **不变**．于是群中对它的所有内同构都不变的子群就是正规子群，所以正规子群又叫做**不变子群**．群中对所有自同构不变的子群，叫做**特征子群**．显然，特征子群也是正规子群．循环群的子群都是特征子群．

共轭也是重要概念，下面是它的基本性质．

假如 a, b 是群 G 中元，如果它们共轭，那末在 G 中最少有一个元 g 存在，使 $a=gbg^{-1}$，也就是说，G 有一个内同构把 b 变成 a．如果 G 是可换，任意元就只能够与它自身共轭．假如 a 与它的所有共轭元相等，那末 a 就在 G 的中心中．

我们很容易证明共轭这个关系是一个等价关系，因此一个群

也可以根据共轭这个关系来分类．这种类我们又叫做**共轭类**．群中与一个元共轭的所有元构成一个共轭类．

假定群 G 的元数为 n，我们把 G 分为共轭类，其中由 1 个元构成的共轭类的个数 c_0 就是 G 的中心 C 的元数，其他的共轭类假如共有 r 个，并且这些类的元数分别是 $c_1, c_2, \cdots, c_r$，那末我们有

$$n=c_0+c_1+c_2+\cdots+c_r,$$

这式叫做 G 的**群等式**，或者叫做 G 的**群方程**．

譬如 S_3 能够分为三个共轭类

$$(1);\ (1\,2\,3),\ (1\,3\,2);\ (1\,2),\ (1\,3),\ (2\,3);$$

即　$S_3=\{(1)\}\cup\{(1\,2\,3),\ (1\,3\,2)\}\cup\{(1\,2),\ (1\,3),\ (2\,3)\}$，

所以 S_3 的群等式为

$$6=1+2+3.$$

同上面一样，假如 H 是群 G 的子群，那末 aHa^{-1} 也是 G 的子群，子群 aHa^{-1} 叫做 H 用 a 得到的**变形**．H 叫做与 aHa^{-1} **共轭**．假如 H 与子群 K 共轭，那末 G 就有一个内同构把 H 变成 K．假如 G 是可换群，那末任意子群只能与它自身共轭，当 $aHa^{-1}=H$ 时，$aH=Ha$，因此我们有

定理 4　设 H 是群 G 的子群．如果 H 与它的所有共轭子群相等，那末 H 就是 G 的正规子群．

下面我们来考虑群 G 中子群 H 的共轭子群的个数．我们知道，因为 H 用它的正规化群 K 中任意元得到的变形仍为 H．又因为对于 K 的左陪集 aK 中任意元 ak，我们有

$$akH(ak)^{-1}=aHa^{-1},$$

并且如果 $aHa^{-1}=bHb^{-1}$，那末 $b\in aK$，所以 G 中 H 的共轭子群的个数等于 K 在 G 的指标 $(G:K)$，因此不大于 H 在 G 的指标 $(G:H)$．假如 G 的元数是 n，那末 H 的共轭子群的个数是 n 的

因数．同样我们容易证明，G 中与元 a 共轭的元的个数等于 G 中所有与 a 能够交换的元形成的子群在 G 的指标．

假如有穷群 G 是它的子群 H 的所有共轭子群的并集，那末 H 的共轭子群的个数是 1，因此 $H=G$．这是因为，如果 H 的共轭子群的个数大于 1，因为子群的单位元都相同，所以 G 的元数就小于 H 的元数与它的共轭子群的个数的乘积，因此 H 在 G 的指标就小于 H 的共轭子群的个数，这与上面已经证明的性质不合．因此，假如 H 是 G 的真子群，那末 G 中有不在 H 的任意共轭子群中的元．

习　题　2.4

1．假定 $G=\{e, a, b, c\}$ 的群表是

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

试证它除了恒等同构外，没有内同构，并且有五个外同构．即克莱茵四元群的自同构群是对称群 S_3，因此可换群的自同构群不一定是可换群．

2．证明对称群 S_3 没有外同构，但有六个内同构，并证明它的自同构群与它自身同构．

3．试证四元数群(§2.3，习题 7)与由矩阵

$$\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad \pm\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix},\quad \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\quad \pm\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$

形成的 8 元群同构．这里 i 是虚数单位．

4．假如 H 是 G 的正规子群，K 是 G 的子群，试证 $H\cap K$ 是 K 的正规子群．

5．假设 H，K 是群 G 的子群，$G\supseteq K\supseteq H$，H 是 G 的正规子群，如果 K/H 是 G/H 的正规子群，试证 K 是 G 的正规子群．

6. 元数是质数 p 的幂 p^n 的群，叫做 **p 群**. 试证 p 群的中心的元数大于 1，也就是说，p 群是有中心的群. 因此 $p^n(n\neq1)$ 元群不是单群.

7. 假如 p 是质数，试证 p^2 元群是可换群.

8. 试证非可换单群与它的内同构群同构.

9. 试证群的中心是特征子群.

10. 试证特征子群这个关系是满足传递律的，也就是说，假如 C 是 B 的特征子群，B 又是 A 的特征子群，那末 C 是 A 的特征子群.

11. 试证包含换位子群的子群是正规子群.

12. 假如 H 是群 G 的子群，K 是 H 的正规化群，试证 aKa^{-1} 是 aHa^{-1} 的正规化群.

13. 假定 H 是群 G 的子群，$G=a_1H\cup\cdots\cup a_nH$，如果 $a_1, \cdots, a_n$ 中与 H 能够交换的只有 $a_1, \cdots, a_m$，那末 H 的正规化群 $K=a_1H\cup\cdots\cup a_mH$. 试用此求{(1), (2 3 4), (2 4 3)}在 S_4 中的正规化群，并求它的共轭子群.

§2.5　同　态

上节同构概念中的可逆映射，假如换成一般的映射，我们就得到它的推广，这节就是讨论这推广概念的基本性质.

定义　假设 M, M' 是两个乘集，σ 是 M 射到 M' 的映射，并且对于 M 中任意两元 a, b,

$$\sigma(ab)=\sigma(a)\sigma(b),$$

那末 σ 叫做 M 射到 M' 的**同态**. 这时，如果 σ 是 M 射到 M' 内的映射，我们就叫 σ 是 M 射到 M' **内的同态**. 如果 σ 是 M 射到 M' 上的映射，我们就叫 σ 是 M 射到 M' **上的同态**，这时我们又说 M 与 M' **同态**，用记号 $M\sim M'$ 表示.

当 σ 是可逆同态时，σ 就是同构，因此同构是同态的特例. 同态这个关系适合自反律，传递律，但不适合对称律，因此同态不是等价关系.

在上面的定义中，如果 $M'\subseteq M$，也就是说，$\sigma(M)\subseteq M$，那末 σ

就叫做 M 的自同态. 假如 σ 是 M 的自同态，当 σ 是可逆映射，并且 $\sigma(M)=M$ 时，也就是说，当 σ 是 M 射到自己上的可逆同态时，那末 σ 就是 M 的自同构.

譬如我们把一个群的每个元都与单位元对应，那就得到群射到单位元群上的同态，这同态又叫做**零同态**. 同样，我们把一个由排列形成的群中元，按照它是奇排列或者是偶排列分别对应于 -1 或者 $+1$，就得到对称群的子群射到由 -1，$+1$ 两个整数形成的群上的同态. 又如我们把每个整数 n 对应于由 a 生成的循环群 (a) 中元 a 的幂 a^n，那就得到加群 Z 射到 (a) 上的同态，当 (a) 是无穷群时，这同态又是同构.

下面我们讨论同态的性质. 因为同构是同态的特例，所以凡是同态所具备的性质，对同构来说也同样成立.

定理 1 假定群 G 与乘集 G' 同态，那末 G' 成群. 这就是说，一个群的同态象也是群.

证明 假定 G' 中任意三元 a', b', c' 的象源分别是 G 中元 a, b, c，那末从 $ab\cdot c=a\cdot bc$，就得到

$$a'b'\cdot c'=a'\cdot b'c'.$$

也就是说，在 G' 中结合律成立. 又由 $ea=a$，我们就有

$$e'a'=a',$$

再由 $a^{-1}a=e$，又有

$$(a^{-1})'a'=e'.$$

也就是说 G' 有单位元 e'，并且 G' 中每个元 a' 也有逆元 $(a^{-1})'$，因此 G' 成群，所以定理成立.

从上面的证明我们还知道，群的同态把单位元 e 变为单位元 e'，元 a 的逆 a^{-1} 变为 a 的象 a' 的逆 $(a')^{-1}$，因此 $(a^{-1})'=(a')^{-1}$，这些都是常常要引用的结果.

要注意的是，上述定理的逆不成立. 这就是说，假如 M, M' 同

态，并且 M' 成群，那末 M 就不一定成群．譬如 M 是所有自然数组成的结合法是加法的乘集，M' 是由 -1，$+1$ 两个整数对于乘法形成的群，显然把偶数变为 1，奇数变为 -1 是 M 射到 M' 上的同态，但这时 M 不是群．当同态是同构时，上定理的逆显然成立．

我们知道群 G 与 G' 同态，其对应关系是多对一的，因此我们要问，G' 中元在 G 中完全象源的元数（即浓度）是否都一致？首先我们来考虑单位元的完全象源．

定理 2　假定群 G 与群 G' 同态，那末 G' 的单位元 e' 在 G 的完全象源 E 是 G 的正规子群，叫做这同态的同态核．

证明　假定 e_i，e_j 是 E 中任意元，因为它们的象都是 e'，所以

$$(e_ie_j^{-1})'=e'\cdot(e')^{-1}=e',$$

于是 $e_ie_j^{-1}\in E$，因此 E 成群．再对于 G 中任意元 a，因为

$$(ae_ia^{-1})'=a'e_i'(a^{-1})'=a'e'(a')^{-1}=a'(a')^{-1}=e',$$

所以

$$aEa^{-1}\subseteq E,$$

于是 E 是正规子群，所以定理成立．

对于任意元的完全象源，我们有

定理 3　假定群 G 与 G' 同态，E 是同态核，G 中元 a 在 G' 中的象是 a'，那末 a' 的完全象源是左陪集 aE．

证明　因为左陪集 aE 中任意元的象都是 $a'e'=a'$，所以 aE 中任意元都是 a' 的象源．再假定 b 的象是 a'，我们从

$$(a^{-1}b)'=(a')^{-1}a'=e,$$

就得到

$$a^{-1}b\in E,$$

于是 $b\in aE$，即 b 在左陪集 aE 中，所以 a' 的完全象源是 aE，因此定理成立．

于是当 $G\sim G'$ 时，G' 中元在 G 中完全象源的元数是一致的．又因为 G 中元素间的关系在 G' 中仍然类似地成立，所以 G' 虽然不能作为 G 的象，但也可以说是 G 的“缩影”．我们研究 G 的缩

影，对 G 的性质必然有所说明，同态的重要也就在此.

假如 G 与 G' 同态，E 是同态核，如果 E 是 G 自身，那末 G' 是单位元群. 如果 E 是单位元群，那末 G 与 G' 同构，即 $G\cong G'$. 假如 $G\cong G'$，那末同态核 E 就是单位元群，因此同态成为同构的必要充分条件是它的同态核是单位元群.

假如 G 是单纯加群，$\sigma(\neq 0)$ 是它的自同态，由定理 1，我们容易得知 $\sigma(G)$ 是 G 中异于单位元群的子群，所以 $\sigma(G)=G$，即 σ 是 G 射到自己上的映射. 再这时同态核显然是单位元群，所以 σ 又是可逆映射，因此 σ 是 G 的自同构. 这就是说，单纯加群的自同态或为零同态，或为自同构.

上面从一个同态出发就得到一个正规子群，那就是它的同态核. 现在我们从 G 的正规子群 H 出发，能否得到 G 的一个同态象？这问题不难解答，只要我们命左陪集 aH 中的任意元与商群 G/H 中元 $\bar{a}$ 对应，就得到 G 射到 G/H 上的同态，因此 G/H 就是我们需要的同态象. 于是我们有

定理 4 假定 H 是群 G 的正规子群，那末 G 与它关于 H 的商群同态，也就是说，

$$G\sim G/H,$$

同态核就是 H，象这样的同态又叫做 G 射到 G/H 上的**自然同态**.

于是我们知道假如 G 有一个同态，它就有一个正规子群；反过来，假如 G 有一个正规子群，它就有一个自然同态. 因此，假如 G 有一个同态，它就有一个自然同态. 说明这两个同态彼此间关系的，有下面的同态基本定理.

定理 5 假定群 G 与 G' 同态，同态核是 E，那末

$$G/E\cong G'.$$

证明 因为 $G\sim G'$，假定这时的同态映射是 $a\to a'$，由上面定

理 3, a' 的完全象源是 a 所在的左陪集 aE. 如果左陪集 aE 用 $\bar{a}$ 表示，命 $\bar{a}$ 与 a' 对应，即 $\bar{a}\to a'$. 因为 $a'=b'$ 时，a, b 同在 E 的一个左陪集；即 $\bar{a}=\bar{b}$, 因此这对应就是 G/E 射到 G' 上的可逆映射. 再因为

$$\bar{a}\bar{b}=\overline{ab}\to(ab)'=a'b',$$

所以 $G/E\cong G'$, 因此定理成立.

于是我们得知，任意同态象可以看成商群，任意同态可以看成是自然同态；也就是说，用正规子群能够决定所有的同态象，正规子群与同态是一对一的，有多少正规子群就有多少同态，这是正规子群也是商群的一个重要性质.

单群就是这样的群，它除自身及单位元群外，没有其他同态象.

假定群 $G\sim G'$, 同态核是 E, H 是 G 的子群，那末 H 在 G' 中的象 H' 也是 G' 的子群，这时 $H\sim H'$. 同态核就是 H 中所有在 E 中的元的集合，即同态核是 $H\cap E$, 于是由上面定理 5, 我们有

$$H/H\cap E\cong H'.$$

当 $H\supseteq E$ 时，

$$H/E\cong H'.$$

习　题　2.5

1. 试证对称群 S_4 关于克莱茵四元群 B_4 的商群 S_4/B_4 与 S_3 同构.

2. 假如群 G 与 G' 同态，它的核是 E, 试证 G 中任意两元在 G' 中有相同的象的必要充分条件是：它们同在 E 的一个陪集中.

3. 试证群 G 的内同构群与 G 关于其中心 C 的商群 G/C 同构. 因此非可换群的自同构群不是循环群.

4. 单群的同态象是单群或者单位元群.

5. 试证 G/E 的任意子群是 H/E, 这里 H 是 G 的子群，并且 $H\supseteq E$.

6. 假定 M, M' 是两个乘集，σ 是 M 射到 M' 上的可逆映射，如果对于 M

中任意元 a, b, $\sigma(ab)=\sigma(b)\sigma(a)$, 那末这 σ 叫做 M 射到 M' 上的**逆同构**. 试证任意群与它自身逆同构.

7. 假定 G 是群, a 是 G 中一元, 试证 $\tau_a(g)=ga$, $g\in G$, 是 G 的一个变换, 并且 G 的所有这样的变换形成一个与 G 逆同构的群.

参 考 文 献

[1] 柔航, 纪念伽罗华诞生150周年, 数学通报, 7(1961), 39~40.

[2] C. Johnson, A mixed non-group, Amer. Math. Monthly, 71 (1964), 785.

[3] (1) Paul Lorenzen, *Ein Beitrag zur Gruppenaxiomatik*, Math. Z., 49 (1944), 313~327.

(2) 陈重穆、金民勇, 关于群的定义, 数学进展, 4 (1958), 127~131.

(3) Slater, Michael, A single postulate for groups, Amer. Math. Monthly, 68 (1961), 346~347.

[4] W. Phillips, On the definition of even and odd permutations, Amer. Math. Monthly, 74 (1967), 1249~1251.

[5] F. Szász, On cyclic groups, Fund. Math., 43 (1956), 238~240.

[6] G. A. Miller, Collected works, vol. 3. University of Illinois Press, Urbona (1946).

[7] G. A. Miller, Groups which contain ten or eleven proper subgroups, Proc. Nat. Acad. Sci. U. S. A., 25 (1939), 540~543.

[8] Humphreys, J. F., On groups satisfying the converse of Lagrange's Theorem, Proc. Cambridge Philos. Soc., 75 (1974), 25~32.

[9] A. Г. 库洛什, 群论(曾肯成、郝炳新译), §9.

[10] L. E. Dickson, Linear groups, with exposition of the Galoisfield theory, 309~310.

[11] W. Feit and J. G. Thompson, Solvability of Groups of odd order, Pacific Jour. of Math., vol. 13, No. 3 (1963).

[12] (1) O. Ore, Some remarks on commutators, Proc. Amer. Math. Soc., 2 (1951), 307~314.

(2) 曾肯成、徐诚浩, 关于两类有限单群中的换位元, 数学进展, 8(1965), 202~208.

[13] 汤璪真, 群之新基本特性, 武汉大学理科季刊, 第8卷, 第1期(1942).

[14] Irving E. Segal, The automorphisms of symmetric group, Bull. Amer. Math. Soc., 46 (1940), 565.

[15] G. W. Miller, On a theorem of Hölder, Amer. Math. Monthly, 65 (1958), 252~254.

第三章

环与体

这章介绍环与体的基本概念，并且详细地叙述环的一些基本性质，最后讨论环中元素的因子分解等问题．这章是以环为主，关于可换体及一般环，后面还要详细讨论．

§3.1 环的概念

在上章我们已经认识了群．群是只有一种结合法的代数系，也就是说，在群中任意两个元只有一种结合法．现在我们来讨论有两种结合法的代数系．在有两种结合法的代数系中，环与体是最基本的．

定义 1 一个非空集合 R，假如它有两种结合法，一种叫做加法(用记号 + 表示)，一种叫做乘法(用记号 · 表示)，并且还满足下面三个条件时，就叫做环：

1° 对于加法成为可换群，叫做 R 的**加群**；

2° 对于乘法成为半群，叫做 R 的**半群**；

3° 对于加法和乘法适合分配律，即对于 R 中任意三元 a, b, c,

$$a(b+c)=ab+ac, \quad (b+c)a=ba+ca.$$

于是环是这样的代数系，其中任意两元对于加、减(加法的逆运算)、乘三个结合法能够任意施行．一个环如果又满足乘法的交

换律，即

$$ab=ba,$$

就叫做**可换环**．只包含有穷个元的环，叫做**有穷环**．

譬如整数集 Z，结合法是普通加法与乘法，成为环，叫做**整数环**．仅一个数 0，结合法是普通加法，乘法，也成为环，叫做**零环**．又用整数组成的所有 n 级矩阵（n 是固定的）形成为环，它不是可换环．一般，假如 R 是环，所有用 R 中元组成的 n 级矩阵形成为非可换环，叫做 R 上的 n 级**全矩阵环**，用记号 R_n 来表示．全矩阵环是非常重要的一类环．

假定 R 是环，$G=\{u_1, \cdots, u_n\}$ 是群，我们容易证明，所有形状象

$$\sum_{i=1}^{n} a_i u_i = a_1 u_1 + \cdots + a_n u_n, \quad a_i \in R$$

的元，根据规定

$$\sum_{i=1}^{n} a_i u_i = \sum_{i=1}^{n} b_i u_i, \text{ 当 } a_i = b_i, \ i=1, \cdots, n;$$

$$\sum_{i=1}^{n} a_i u_i + \sum_{i=1}^{n} b_i u_i = \sum_{i=1}^{n} (a_i + b_i) u_i,$$

$$\left(\sum_{i=1}^{n} a_i u_i\right)\left(\sum_{j=1}^{n} b_j u_j\right) = \sum_{i,j=1}^{n} a_i b_j u_i u_j,$$

形成为环，叫做 G 关于 R 的**群环**，用 $R[G]$ 表示[1]．

下面我们给出一个有穷环的例子．

我们知道 $Z-(n)=\{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ 是加群，它的加法是 $\bar{a}+\bar{b}=\overline{a+b}$．现在我们再来规定它的乘法为

$$\bar{a}\bar{b}=\overline{ab},$$

也就是说，当 $ab\equiv c(n)$ 时，$\bar{a}\cdot\bar{b}=\bar{c}$．这规定是一意的，因为假如 $a\equiv a'(n)$，$b\equiv b'(n)$，那末 $ab\equiv a'b'(n)$．我们容易证明 $Z-(n)$ 对于乘法成为半群，并且还适合分配律，因此它成为一个有穷环，$\bar{0}$

是它的零元，$\bar{1}$是它的单位元.

环 R 的子集 S，假如对于 R 的两种结合法形成为环，那末 S 就叫做 R 的**子环**，R 叫做 S 的**扩张环**. 环的一个子集成为子环，只要它对加法成群，对乘法是闭合的就行了，因为其他条件显然都适合.

有穷环显然只能有有穷个子环. 反过来也成立，即一个环如果只有有穷个子环，那末这环是有穷环[2].

环可以看成是自身的子环，异于自身的子环叫做**真子环**. 任意环都有只由一个零元形成的零环作它的子环. 同群的情况一样，环中与所有元能够交换的全部元形成子环，叫做环的**中心**. 显然可换环的中心就是它自身.

上面说明了环及子环的概念，并且给出了一些例子，现在我们来讨论环的一些基本概念及基本性质.

因为环 R 对于加法成群，也就是说 R 是加群，所以我们把它的单位元写成零元 0，元 a 的逆元写成 a 的负元 $-a$. 在环中用加法表示的各种性质，也就是加群的各种性质，由第二章可以直接推得. 下面我们只讨论与乘法有关的各种性质.

零元及负元在加法中的地位由加群的性质已很清楚，它们与乘法的关系有

1° $0\cdot a=a\cdot 0=0$,

2° $(-a)\cdot b=a\cdot(-b)=-ab, \quad (-a)(-b)=ab$,

式中 a, b 是环 R 中任意元.

这是因为由分配律

$$0\cdot a+0\cdot a=(0+0)a=0a$$

就得到

$$0\cdot a=0,$$

同样 $a\cdot 0=0$，因此 1° 得证.

又因为

$$(-a)b+ab=(-a+a)b=0b=0,$$

所以 ab 是 $(-a)b$ 的负元，也就是说，$(-a)b=-ab$. 同样，$a(-b)=-ab$.

再因为

$$(-a)(-b)=-(-a)(b)=-(-ab)=ab,$$

因此 2° 得证.

此外，我们容易知道，

$$c(a-b)=ca-cb, \quad (a-b)c=ac-bc,$$

这就是说，在环中对于减法的分配律也是成立的.

于是环 R 中元施行加法，减法，乘法等运算时，与普通代数中数的情况一样. 但必须注意，乘法的先后顺序不一定可以颠倒，除法(乘法的逆运算)在 R 中不一定可以施行，因此乘法的消去律也不一定成立，这就是说，从 $a\cdot b=a\cdot c$ 或者 $b\cdot a=c\cdot a$，当 $a\neq 0$ 时，我们不一定能够得到 $b=c$. 也就是说，从 $a\cdot b=0$，我们不一定能够得到 $a=0$ 或 $b=0$.

假如 a 是环 R 的元，如果 R 中有一元 $b\neq 0$ 存在，使 $ab=0$ $(ba=0)$，那末 a 就叫做 R 的**左(右)零因子**，有时 a 又叫做 b 的**左(右)零化元**. 一元如果是左零因子，同时又是右零因子，就叫做**零因子**. 非零环的零元是当然的零因子. 一般，环中除零元外，可能还有其他零因子.

譬如在整数环 Z 上的 2 级全矩阵环 Z_2 中，非零的元

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}$$

都是零因子，这是因为

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}=0, \quad \begin{pmatrix} 0 & 0 \\ b & -a \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}=0.$$

定义 2 假定环 R 中除零元外既没有左零因子，也没有右零因子，那末 R 就叫做**无零因子环**；可换无零因子环又叫做**整环**.

譬如整数环 Z 是整环. 显然，环成为无零因子环的必要充分条件是对于其中任意两元 a, b，如果 $ab=0$，那就有 $a=0$ 或 $b=0$. 再假如 R 是无零因子环，由 $ab=ac$ 或 $ba=ca$，这里 $a\neq 0$，就可以得到 $b=c$，这是因为 $a(b-c)=0$ 或 $(b-c)a=0$，而 $a\neq 0$，所以 $b-c=0$，即 $b=c$. 因此，在 R 中乘法的消去律成立. 反过来，假如在环 R 中乘法的消去律成立，如果其中两元 a, b 的积 $ab=0$ 而 $a\neq 0$，我们由 $ab=a0$ 就得到 $b=0$，因此 R 是无零因子环. 于是我们又得知，环成为无零因子环的必要充分条件是它满足乘法的消去律.

环中元 a，如果 $a^n=0$，这里 n 是正整数，那末 a 叫做**幂零元**. 零元是幂零元，非零的幂零元是零因子. 显然，在无零因子环中零元是唯一的幂零元，它没有非零的幂零元. 但反过来不一定成立，即在没有非零的幂零元的环中可能有零因子. 譬如在 $Z-(6)$ 中，2, 3, 4 都不是幂零元，但却都是零因子.

一个环，其中任意元如果都是幂零元，就叫做**幂零元环**.

定理 1 可换环 R 中所有幂零元形成一个幂零元环.

证明 假定 a, b 是 R 中任意两个幂零元，$a^m=0$, $b^n=0$，因为

$$(a-b)^{m+n}=a^{m+n}-C_1^{m+n}a^{m+n-1}b+\cdots+C_n^{m+n}a^m(-b)^n$$
$$+C_{n+1}^{m+n}a^{m-1}(-b)^{n+1}+\cdots+(-b)^{m+n}=0,$$
$$(ab)^m=a^mb^m=0,$$

即 a, b 的差 $a-b$ 及积 ab 又都是幂零元，所以 R 中所有幂零元形成为环，于是定理成立.

下面我们来讨论环中关于乘法的单位元及逆元.

我们知道，环对乘法只能成为半群，所以在环的定义中，并不要求对乘法要有单位元，但在许多环中往往有这种元存在.

定义 3 假如环 R 中有元 $e_L(e_R)$，它对于 R 中任意元 a 有 $e_La=a(ae_R=a)$，那末 $e_L(e_R)$ 就叫做 R 的**左(右)单位元**. 假如 R 中有元 e，它既是左单位元，同时又是右单位元，即对于 R 中任意元 a 有 $ea=ae=a$，那末 e 就叫做 R 的**单位元**，这时 R 叫做**有单位元的环**.

譬如整数环 Z 是有单位元的环，它的单位元就是 1. 所有的偶数也成为环，叫做**偶数环**，但它没有单位元. 当 R 有单位元 e 时，n 级全方阵环 R_n 也有单位元，这单位元就是单位矩阵$\begin{pmatrix} e & & \\ & \ddots & \\ & & e \end{pmatrix}$.

要注意的是，假如环有单位元，它的子环不一定有单位元；如果它的子环也有单位元，这两个单位元不一定一致. 譬如所有形状象$\begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix}$，$a$ 是整数的矩阵形成 Z_2 的子环，显然$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$是它的单位元，但不是 Z_2 的单位元. 但环的零元与子环的零元是一致的. 在异于零的环中，单位元不是零元.

假如环 R 有左单位元 e_L，同时又有右单位元 e_R，那末，

$$e_Le_R=e_L=e_R,$$

也就是说，e_L 或 e_R 是 R 的单位元. 因此在有单位元的环中，左单位元就是右单位元，也就是单位元，并且单位元是唯一的. 在没有单位元的环中，左单位元，右单位元不能同时存在. 假如环 R 只有一个左单位元 e_L，那末 e_L 就是 R 的单位元，这是因为对于 R 中任意元 a，显然 e_L+ae_L-a 又是 R 的左单位元，所以 $e_L+ae_L-a=e_L$，因此 $ae_L=a$，这就是说，e_L 是 R 的右单位元，所以它是 R 的单位元.

一个环可能有不只一个左单位元而没有右单位元，同样也可能有不只一个右单位元而没有左单位元. 譬如所有形状象$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$

的矩阵形成的环，它没有右单位元，但有无穷多个左单位元

$$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix},$$

这里 a, b, c 都是整数．同样，所有形状象$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$的矩阵形成的环没有左单位元，但有无穷多个右单位元

$$\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}.$$

又单位元显然不是零因子，但左(右)单位元就不一定，譬如上面的左单位元$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$就是右零因子，这是因为

$$\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

环中元 a，如果 $a^2=a$，那末 a 就叫做**幂等元**．显然，左(右)单位元是幂等元．零元当然满足上面幂等元的条件，但我们不把它看成幂等元，因此我们所说的幂等元是异于零的元．幂等元可能是零因子，因此幂等元不一定是单位元．

幂等元 e 假如不是左零因子，同时又不是右零因子，那末它就是单位元．这是因为，从 $e^2=e$，我们有 $e^2a=ea$，即 $e(ea-a)=0$，所以 $ea=a$，同样 $ae=a$，因此 e 是单位元．于是在无零因子环中，左(右)单位元都是单位元，假如它有幂等元，因为幂等元是单位元，那末单位元就是唯一的幂等元了．

一环，其中任意非零的元都是幂等元的，就叫做**布尔**(G. Boole, 1815～1864)**环**．譬如 $Z-(2)$ 就是布尔环．

纵然环 R 有单位元 e，但当 $a\in R$ 时，对乘法，a 也未必就有左(右)逆元．

定义 4 假设环 R 有单位元 e，对于 R 中元 a，如果有元 $a_L^{-1}(a_R^{-1})$ 存在，使 $a_L^{-1}a=e(aa_R^{-1}=e)$，那末 $a_L^{-1}(a_R^{-1})$ 就叫做 a 的**左(右)逆元**．如果有元 a^{-1}，它既是 a 的左逆元，同时又是 a 的右逆

元，即 $a^{-1}a=aa^{-1}=e$，那末 a^{-1} 就叫做 a 的**逆元**.

在有单位元的环中，每一元未必都有逆元. 有逆元的元，叫做**可逆元**. 譬如零元 0，它就没有逆元. 单位元 e 的逆元就是它自身. 如果 a 有逆元 a^{-1}，那末 a^{-1} 的逆元就是 a；如果 a 有逆元 a^{-1}，b 有逆元 b^{-1}，那末 ab 的逆元就是 $b^{-1}a^{-1}$.

零元固然没有逆元，就是零因子同样也没有逆元. 这是因为，假如 a 是零因子，$ab=0$，$b\neq 0$，如果 a 有逆元 a^{-1}，那末 $a^{-1}ab=0$，于是 $eb=b=0$，这与假设不合，所以 a 没有逆元. 因此，如果 a 有逆元，那末它就不是零因子.

同单位元的性质类似，如果 a 有左逆元 a_L^{-1}，同时又有右逆元 a_R^{-1}，那末它就有逆元 $a^{-1}=a_L^{-1}=a_R^{-1}$，这是因为

$$a_L^{-1}=a_L^{-1}e=a_L^{-1}aa_R^{-1}=ea_R^{-1}=a_R^{-1}.$$

因此一个元 a 如果有逆元，它的左逆元就是右逆元也就是逆元，并且它的逆元是唯一的. 一元可能有几个左逆元而没有右逆元，同样也可能有几个右逆元而没有左逆元[3]. 但在无零因子环中，如果 a_L^{-1}，a_R^{-1} 有一存在，譬如说 a_L^{-1}，因为 $a_L^{-1}a=e$，$a_L^{-1}(aa_L^{-1}-e)=0$，所以 $aa_L^{-1}=e$，于是 $a_L^{-1}=a_R^{-1}$，也就是说，这时 a_R^{-1} 存在，因此 a^{-1} 也存在.

定理 2 在有单位元的环 R 中，所有可逆元对乘法形成为群 G.

证明 因为两个可逆元的乘积仍然是可逆元，所以 G 适合群定义(§ 2.1)的条件 1°. 由环的定义，显然 G 适合群定义的条件 2°. R 的单位元也就是 G 中乘法的单位元，又 a^{-1} 就是 a 的逆. 因此 G 成群，所以定理得证.

譬如在整数环 Z 中，可逆元只有 1，-1 两数，它们对乘法显然成群. 又如在全矩阵环 Q_n 中，任意 n 级满秩矩阵都有逆矩阵，因此 Q_n 中所有 n 级满秩矩阵对乘法成为群. 再如在环 $Z-(6)$

中. $\bar{2}, \bar{3}, \bar{4}$ 都是零因子，因此它们都不是可逆元；$\bar{1}$ 的逆元是 $\bar{1}$，$\bar{5}$ 的逆元是 $\bar{5}$，这是因为 $\bar{5}\bar{5}=\bar{1}$. 因此在 $Z-(6)$ 中所有可逆元形成元数为 2 的循环群.

上面所说的单位元以及逆元的性质，只是由环对乘法是半群这性质推得的，因此一个半群也有这些性质.

习 题 3.1

1. 假定 R 是实数集. 加法 $+$ 是普通的加法，但乘法 $\times$ 是

$$a\times b=|a|b,$$

这时 R 是否成环？

2. 假设 R 是所有有理数对 (a_1, a_2) 的集合，它们的结合法是

$$(a_1, a_2)+(b_1, b_2)=(a_1+b_1, a_2+b_2),$$

$$(a_1, a_2)\cdot(b_1, b_2)=(a_1b_1, a_2b_2),$$

那末 R 是否成环？它有无零因子？是否有单位元？那些元有逆元？

3. 假定 R 是有单位元 1 的环，

$$a\oplus b=a+b-1, \quad a\odot b=a+b-ab,$$

试证 R 对结合法 $\oplus$, $\odot$ 也形成一个有单位元的环.

4. 假设

$$a=\begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & \ddots \end{pmatrix}, \quad b=\begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & 1 & \ddots & \\ & & \ddots & \end{pmatrix}, \quad e=\begin{pmatrix} 1 & & \\ & 1 & \\ & & \ddots \end{pmatrix}$$

是二个无穷级矩阵，试证

$$ab=e, \quad ba\neq e,$$

即在由整数组成的无穷级矩阵形成的环中，元 a 有右逆但没有左逆. 并求证 a 是左零因子而 b 是右零因子.

5. 假如 R 不是零环，a 是 R 的左(右)零因子，那末 a 没有左(右)逆元，并且 a 或是没有右(左)逆元，或是最少有两个右(左)逆元. 一元如果它只有一个右逆元，那末它也有逆元.

6. 假如 e 是环 R 的左单位元，如果 R 没有右零因子，那末 e 是 R 的单位元.

7. 在环 R 中，假如 a 与 b 可换，即 $ab=ba$，那末 a 与 b^{-1}，$-b$，nb*)（n 为整数）也都可换；又假如 a 与 b，c 都可换，那末它与 $b+c$，bc 也都可换.

8. 假定 R 是有单位元的环，C 是 R 的中心，E 是全矩阵环 R_n 的单位元，试证 R_n 的中心是 CE.

9. 假定环 R 没有非零的幂零元，试证 R 的幂等元都在它的中心里面.

10. 试证布尔环是可换环.

§3.2　体的概念

在近世代数中，除了群、环外，体是一个最基本的概念.

定义　一个环 F，假如含有非零的元（即至少包含两个元），并且所有非零的元对乘法形成群，就叫做**体**，有时又叫做**可除环**. 这对乘法形成的群，又叫做 F 的**乘群**. 当 F 是可换时，F 就叫**可换体**，或者叫做**域**.

于是我们得知，体有加法、乘法两种运算，并且所有元对加法成加群（可换群），所有非零元对乘法成群，但不一定是可换群. 联系加法与乘法的就是分配律. 因此体中任意两元能够任意施行加、减、乘、除，只是零元不能除任意元.

一个体 F 至少包含两个元，一个是加群的零元，一个是乘群的单位元，每个非零的元都有逆元，所以它不是零因子. 于是 F 是无零因子环. 因此当 F 是可换体时，它又是整环.

体是无零因子环，它的逆一般不成立，但对有穷环是成立的，即

定理 1　元数大于 1 的有穷无零因子环是体.

---

*) nb 的意义是 n 个 b 相加，不是 R 中两个元的乘积，因为 n 是整数，不一定在 R 中，即令在 R 中，$n\cdot b$ 也不一定就是 nb. 但当 R 有单位元 e 时，nb 确是 R 中两元的乘积，这是因为，

$$nb=n(eb)=eb+\cdots+eb=(e+\cdots+e)b=ne\cdot b.$$

证明 由§3.1,环中非零元满足乘法的消去律.再由§2.1定理3,它对除法是闭合的,因此环中所有非零元对乘法成群. 所以这环成体. 定理得证.

于是有穷环如果不是体,它就含有零因子.

1964年根山(N.Ganesan)给出了有穷环的元数与其所含零因子的个数之间一些关系[4],但有穷环详细的构造现在我们还不完全清楚.

我们知道,环成为体只要它的所有非零元对乘法能够成群,因此由§2.1定理2,假如对于环R中任意两元$a(\neq 0)$, b, 方程$ax=b$, $ya=b$在R中有解,那末R就是体. 下面我们来证明上面两个方程只要一个有解就行了.

定理2 环R成体的必要充分条件是: 对于R中任意两元$a\neq 0$, b,方程$ax=b$(或$xa=b$)在R中有解.

证明 因为条件的必要性显然成立,我们只证明充分性.

假定a, b是R中任意非零的两元, 从$ax=b$, $by=x$, 我们有

$$aby=ax=b,$$

于是$ab\neq 0$, 这就是说, R中任意非零的两元的积仍然是非零的元,因此R是无零因子环. 又由$ae=a$,我们有

$$a(e^2-e)=0,$$

于是$e^2=e$,这就是说,e是无零因子环R的幂等元,所以e是R的单位元. 再从$aa'=e$,所以a'是a的右逆元,但R是无零因子环,因此a'也是a的逆元. 于是R中所有非零的元对乘法成群,因此R是体,充分条件成立.所以定理得证.

现在我们给出一些例子.

譬如有理数集Q成为体,叫做**有理数体**; 所有有理复数$a+bi$(a, b是有理数)集也成为体,叫做**高斯**(C. F. Gauss, 1777～1855)**数体**. 同样,实数集,复数集都成为体,分别叫做**实数体**, **复数体**.

只包含有穷个元的体，叫做**有穷体**．将来(§4.10)我们还可以知道，任意有穷体都是可换体．下面我们举一个有穷体的例子．

假设 p 是质数，那末 $Z-(p)$ 就是元数为 p 的有穷体．这是因为，假如 $\bar{a}$, $\bar{b}$ 是 $Z-(p)$ 中任意两元，如果 $\bar{a}\bar{b}=\bar{0}$，也就是说，$ab\equiv 0(p)$，根据 p 是质数的假设，我们有 $a\equiv 0(p)$ 或 $b\equiv 0(p)$，于是 $\bar{a}=\bar{0}$ 或 $\bar{b}=\bar{0}$，所以 $Z-(p)$ 是无零因子环．因此由定理 1，$Z-(p)$ 成体．但数是服从乘法的交换律的，所以 $Z-(p)$ 是可换体．要注意的是，当 n 不是质数时，$Z-(n)$ 有非零的零因子，因此它不成体，于是 $Z-(n)$ 成为体的必要充分条件是 p 为质数．

我们还举一个体的例子，这是 1843 年汉弥尔顿提出的，是历史上第一个不可换体的例子．

我们先介绍一种比复数更广泛，叫做**四元数**的数：

$$ae+bi+cj+dk,$$

这里 a, b, c, d 是实数．为了简便，象 $ae+0i+0j+0k$ 我们写成 ae, $0e+0i+1j+0k$ 写成 j 等等．我们希望所有这样的实四元数能够成为环．首先我们规定 e, i, j, k 的乘法表

	e	i	j	k
e	e	i	j	k
i	i	$-e$	k	$-j$
j	j	$-k$	$-e$	i
k	k	j	$-i$	$-e$

再规定它们一般的相等，相加及相乘等关系：

1．$ae+bi+cj+dk=a'e+b'i+c'j+d'k$，当：

$$a=a',\ b=b',\ c=c',\ d=d',$$

2．$(ae+bi+cj+dk)+(a'e+b'i+c'j+d'k)$

$$=(a+a')i+(b+b')j+(c+c')j+(d+d')k,$$

3. $(ae+bi+cj+dk)(a'e+b'i+c'j+d'k)$是将这式依分配律展开，然后把各项的实系数合并，譬如令$(ai)(bj)=ab(ij)$，再用上面规定的乘法结果代入所得到的四元数.

对这样规定的结合法，我们很容易证明上面的所有实四元数形成为环，它是非可换环，e是它的单位元；再因为

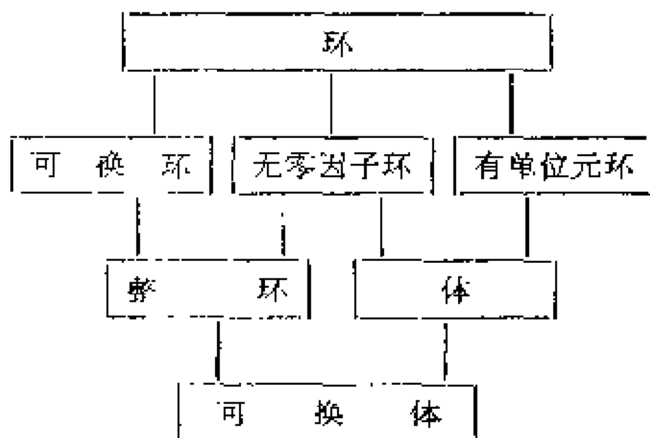
$$(ae-bi-cj-dk)(ae+bi+cj+dk)=(a^2+b^2+c^2+d^2)e,$$

所以对于每个非零元$ae+bi+cj+dk$都有逆元

$$(a^2+b^2+c^2+d^2)^{-1}(ae-bi-cj-dk),$$

因此它们形成为体，叫做**四元数体**，它是非可换体.

上节及这节讨论的环、体间关系，可以用图式表示如下：



习 题 3.2

1. 试作由两个元形成的体.
2. 假如n不是质数，那末$Z-(n)$就不成为体，为什么？
3. 试证体的中心是可换体.
4. 试证所有系数是复数的四元数只能形成为环而不能形成为体.
5. 假定a, b, c是四元数环中任意元，试证$(ab-ba)^2c=c(ab-ba)^2$.

§3.3 同态，同构

我们已经知道群的同态、同构，这节我们把它推广到环、体上

面来.

定义 假定 R, R' 是两个环, σ 是 R 射到 R' 的映射, 如果对于 R 中任意元 a, b, 我们有

$$\sigma(a+b)=\sigma(a)+\sigma(b),\quad \sigma(ab)=\sigma(a)\sigma(b),$$

那末映射 σ 就叫做 R 射到 R' 的**同态**. 如果 σ 是 R 射到 R' 内的映射, 我们就叫 σ 是 R 射到 R' **内的同态**, 如果 σ 是 R 射到 R' 上的映射, 我们就叫 σ 是 R 射到 R' **上的同态**, 这时我们又说 R 与 R' **同态**, 用记号 $R\sim R'$ 表示. 如果 σ 更是可逆的, 它就叫做**同构**, 这时 R 叫做与 R' **同构**, 用 $R\cong R'$ 表示.

譬如任意环 R 都与零环同态, 因为我们把 R 中所有元都与零元对应就是零同态. 又如环 $Z-(8)=\{\bar{0}, \bar{1}, \cdots, \bar{7}\}$ 与 $Z-(4)=\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ 同态, 这是因为由计算可以验证, 下面的对应是它们的同态:

$$\bar{0}\to\bar{0}',\ \bar{1}\to\bar{1}',\ \bar{2}\to\bar{2}',\ \bar{3}\to\bar{3}',$$

$$\bar{4}\to\bar{0}',\ \bar{5}\to\bar{1}',\ \bar{6}\to\bar{2}',\ \bar{7}\to\bar{3}'.$$

再假如 K 是高斯数体, K' 是由所有形状象$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$的矩阵形成的体, 其中 a, b 是有理数, 命

$$a+bi\to\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

显然这对应是 K 射到 K' 上的可逆映射; 再因为

$$(a+bi)+(c+di)=(a+c)+(b+d)i,$$

$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i,$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}+\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\cdot\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix},$$

所以这映射又是同构，因此 $K\cong K'$.

同讨论群的情形一样，同构关系是等价关系，同态关系不是等价关系．同态满足自反律，传递律，但不满足对称律．

两个同构的环除了记号外构造完全一样，也就是说，它保持原来环中用加法，乘法两种结合法表示的一切代数性质，所以我们有时也把同构的环看成是相同的环．但同态就不是这样，它不一定保持原有的性质．譬如 $R\sim R'$ 时，假如 R 有单位元，那末 R' 也有单位元，但反过来就不一定成立．再假如 R 是可换，那末 R' 也是可换，但反过来又不一定成立．又假如 R 是无零因子环，R' 中可能有零因子；反过来，假如 R' 是无零因子环，R 中也可能有零因子，因此 R 是整环时，R' 不一定是整环；反过来，R' 是整环时，R' 也不一定是整环，譬如 $Z\sim Z-(6)$，但 Z 是整环而 $Z-(6)$ 有零因子．又如所有形状象 $\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$ 的矩阵，这里 a, b, c 都是整数，形成环 R，根据 $\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\to a$，我们容易验证它与整数环 Z 同态，即 $R\sim Z$，这时 R 是非可换环，并且有非零的零因子．

因为环的同态也是把环看成加群时的同态，所以它把零元变为零元，一元的负元变为这元的象的负元，因此两元的差变为它们的象的差．又由定义，我们容易得知环的同态把幂零元变为幂零元，幂等元变为幂等元．假如环有单位元，那末单位元也变为单位元，因此一元的逆又变为这元的象的逆．

同群一样，环也有自同态、自同构．我们容易得知，整数环及有理数体的自同构都只是恒等同构．$a+bi\to a-bi$ 是复数体的自同构．由可逆元 a 决定的自同构 $x\to axa^{-1}$，叫做内(自)同构，不是内(自)同构的自同构，叫做**外(自)同构**．对于任意内同构不变的子环，叫做**不变子环**．我们知道，在一个非可换体中，它自身及包含在它中心里面的子体都是不变子体．反过来也成立，也就是说，

在一个非可换体中,不变子体只有它自身及包含在它中心的子体.这个逆是 1947 年卡登 (H. Cartan, 1906～) 就关于中心是有穷次体 (§ 4.4) 的特殊情形首先证明, 1949 年布劳尔 (R. Brawer, 1901～), 华罗庚(1910～)同时把它推广到一般体, 因此这个逆就叫做卡登–布劳尔–华罗庚定理[5].

我们将来(§ 3.6)还可以证明,体的同态都是同构. 也就是说,在上面定义中, R, R' 如果都是体,我们可以证明 σ 是可逆的.

假定 G 是加群, σ, τ 是它的自同态, 因为 $\sigma\tau(a)=\sigma(\tau(a))$, 由 § 2.4 我们得知, σ, τ 的乘积 $\sigma\tau$ 是 G 的自同态, 现在我们更规定

$$(\sigma+\tau)(a)=\sigma(a)+\tau(a),$$

显然 σ, τ 的和 $\sigma+\tau$ 也是 G 的自同态, 并且容易证明, 加法的交换律,结合律及分配律都成立. 再我们又有

$$0(a)=0, \quad -\sigma(a)=\sigma(-a),$$

因此 G 的所有自同态形成有单位元的环,叫做 G 的**自同态环**.

显然,单位元群的自同态环是零环. 无穷循环群的自同态环与整数环 Z 同构. n 元循环群的自同态环与 $Z-(n)$ 同构. 因此元数是质数 p 的循环群的自同态环就是可换体 $Z-(p)$. 一般我们有:

定理 1　元数大于 1 的单纯加群的自同态环是体.

这是因为由 § 2.5 我们得知, 单纯加群的异于零的自同态是自同构.

假如把环看成加群,那末它也有自同态环,即任意一个环都有自同态环. 但要注意的是, 这里所说的自同态是把环看成加群时的自同态,并不是环的自同态. 因为

$$(\sigma+\tau)(ab)\neq(\sigma+\tau)a\cdot(\sigma+\tau)b,$$

所以环的两个自同态 σ, τ 的和 $\sigma+\tau$ 一般不再是环的自同态, 因此环的所有自同态不能形成为环.

假定 R 是环，a 是其中一元，显然映射 $\sigma_a(r)=ar$ 是把 R 看成加群时的自同态，因为 $\sigma_{a+b}=\sigma_a+\sigma_b$，$\sigma_{ab}=\sigma_a\cdot\sigma_b$，所以所有这些自同态 σ_a 形成环 R'．根据定义，我们容易证明，$a\to\sigma_a$ 是 R 射到 R' 上的同态．当 R 有单位元 e 时，这同态又是同构，这是因为由 $\sigma_a=\sigma_b$，我们就有 $ar=br$，因此便得到 $ae=be$，即 $a=b$．于是我们有

定理 2 假定 R 是有单位元的环，a 是其中一元，$\sigma_a(r)=ar$，那末 R 与所有自同态 σ_a 形成的环同构．

将来(§3.4 习题 3)我们还知道，一个没有单位元的环可以看成为一个有单位元环的子环，或者说，一个没有单位元的环可以嵌入一个有单位元的环．这样我们就得到下面与 §2.4 中卡莱定理类似的定理．

定理 3 任意环与某环的自同态环的子环同构．

下面是我们常常引用的**挖补定理**．

定理 4 假设 R' 与 S 是两个没有公共元的环，并且 S 含有一个与 R' 同构的子环 R，那末我们有一个包含 R' 并且与 S 同构的环 S'，这就是说，这时我们简直就可以把 R' 看成是 S 的子环．

这定理的含义我们可以用下面的图形(图 3.1)来表示．

证明 我们命

$$S'=R'\cup(S-R),$$

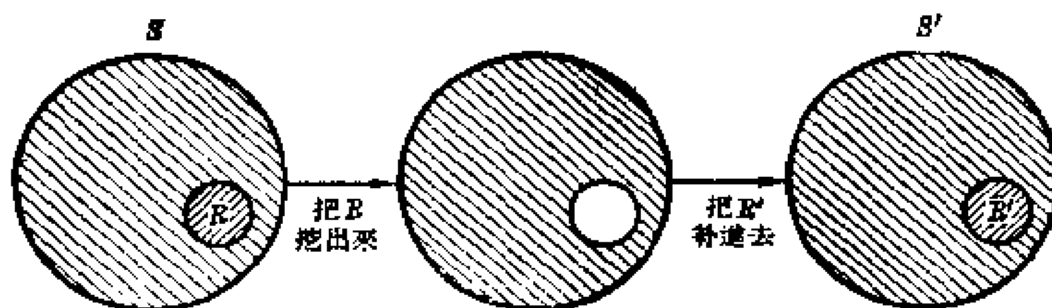


图 3.1

也就是说，S' 是 S 中把 R 挖去换成 R' 的集合．因为 $S\cap S'=S-R$，我们命 $S-R$ 中元与它自身对应，R 中元与 R' 中元的对应关系不变(根据假设 R 与 R' 同构)．我们就得到 S 射到 S' 上的可逆映射．假定这映射用 $a\to a'$ 表示，这时我们规定 S' 的结合法是

$$a'+b'=(a+b)', \quad a'b'=(ab)',$$

显然 S' 是环，并且其中 R' 的结合法与原来的一样，没有变动，因此 S' 是 R' 的扩张环．再我们容易知道 $a\to a'$ 就是 S 射到 S' 上的同构，所以 $S\cong S'$，因此定理成立．

同 §2.5 习题 6 一样，关于环我们常常引用与同态类似的另一种映射．假定 σ 是环 R 射到 R' 上的映射，并且对于 R 中任意元 a，b，

$$\sigma(a+b)=\sigma(a)+\sigma(b), \quad \sigma(ab)=\sigma(b)\sigma(a),$$

那末 σ 叫做 R 射到 R' 上的**逆同态**，R 叫做与 R' 逆同态．当 σ 是可逆时，σ 就叫做 R 射到 R' 上的**逆同构**，这时 R' 又叫做 R 的**逆环**．显然，环与它的逆环的逆环同构．假如环是可换，那末逆同态就是同态，因此对于可换环，我们就不需要逆同态这个名词了．

1949 年华罗庚发表了下面的定理，在这里我们只叙述这定理，它的证明我们就不谈了[6]．

假定 σ 是环 R 射到 R' 的映射，它使 R 中两元的和与这两元在 R' 中象的和对应，两元的积与这两元的象的积对应，那末 R 中两元在 R' 中象的积的顺序只有两种可能，一是都与它们的象源的积的顺序一致，一是都与象源的积的顺序相反．不存在某些两元的象的积的顺序与象源的积的顺序一致，而另一些则相反，也就是说，这时 σ 是 R 射到 R' 上的同态或者是逆同态．

习 题 3.3

1．假如 R 是环，S 是非空集合，并且对于加法与乘法都是闭合的，如果

有一个 R 射到 S 上的映射 σ 存在，它保持元素间的和及积的关系，那末 S 也是环(参看 §2.5 定理 1)．又假如 R 是体，S 是否仍然是体?

2．试证所有整数形成的加群与所有偶数形成的加群同构，但整数环不与偶数环同构．

3．试证体的乘群不与它的加群同构．

4．试证 $a+bi\to a-bi$ 是复数体的自同构．

5．有理数加群的自同态环与有理数体同构．

6．试证所有形状象

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix},\quad a,\ b,\ c,\ d \text{都是实数}$$

的 2 级矩阵形成一个与四元数体同构的体．

7．假定 K 是四元数体，$\alpha=ae+bi+cj+dk$，$\alpha'=ae-bi-cj-dk$，试证 $\alpha\to\alpha'$ 是 K 的自逆同构．

8．假定环 R 有单位元，$\tau_a(r)=ra$，试证所有 τ_a 形成与 R 逆同构的环．

§3.4　商　　体

环所以不能成为体，是因为它的元不一定都有逆元．现在我们要问，可否把这些逆元以及与逆元的乘积都添入使它成为体?也就是说，环是否可以扩张成为体?或者说一个环能否嵌入于一体?

我们知道，整数集 Z 只成为整环，它不能成为体，因为它的元除 1 及 -1 两数外，都没有逆元．如果我们把这些逆元以及与逆元的乘积也就是把所有由整数做成的商添入，那就成为有理数体 Q．现在我们仿照这方法，从可换环 R 做出这些逆元也就是这些“商”，添加于 R 使它成为包含 R 的可换体，这就是说，对于一个可换环，我们可以做一个可换体把所给的环嵌入．我们分两步来进行．首先假设有一个包含 R 的已知体 K，在这 K 中如何去找这些商，使它们成为包含 R 的可换体；其次，在一般情况下，假定包

含 R 的体不是已知，如何去从一个可换环做出商成为包含它的可换体.

我们知道，假如 a, b 是体中非零的元，如果 $ab=ba$，那末 $ab^{-1}=b^{-1}a$，这就是说，b 左除 a 与 b 右除 a 结果是一致的. 因此我们就简单地叫它做 b 除 a 的商，用 $\frac{a}{b}$ 来表示，即

$$\frac{a}{b}=ab^{-1}=b^{-1}a^{*)}.$$

定理 1 假设 K 是包含可换环 R 的体，那末 K 中所有的商 $\frac{a}{b}$, $b\neq 0$, a, $b\in R$, 形成一个包含 R 的可换体 F，这 F 叫做 R 的**商体.**

证明 首先我们容易得知，对于这些商，下面的计算法则都能够成立：

1° $\frac{a}{b}=\frac{c}{d}$，当 $ad=bc$,　　2° $\frac{ca}{cb}=\frac{ac}{bc}=\frac{a}{b}$,

3° $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$,　　4° $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$.

这是因为，如果 $\frac{a}{b}=\frac{c}{d}$，即 $b^{-1}a=cd^{-1}$，那末 $ad=bc$，所以 1° 成立. 2° 可由 1° 直接推得. 再因为

$$\begin{aligned}\frac{ad+bc}{bd}&=(bd)^{-1}(ad+bc)=(bd)^{-1}(ad)+(bd)^{-1}(bc)\\&=\frac{ad}{bd}+\frac{bc}{bd}=\frac{a}{b}+\frac{c}{d},\end{aligned}$$

$$\frac{a}{b}\cdot\frac{c}{d}=b^{-1}ad^{-1}c=b^{-1}d^{-1}ac=(bd)^{-1}\cdot ac=\frac{ac}{bd},$$

所以 3°, 4° 都成立.

因为商 $\frac{0}{a}=0$，所以 0 也是商，再因为

*) b 虽然在 R 中，但 b^{-1} 不一定在 R 中，因此 $ab^{-1}=b^{-1}a$ 也不一定在 R 中.

$$\frac{a}{b}+\frac{-a}{b}=\frac{a+(-a)}{b}=\frac{0}{b}=0,$$

所以 $\frac{a}{b}$ 的负元是商 $\frac{-a}{b}$. 因此所有这些商，也就是 F，成为加群.

又因为 $\frac{a}{a}=e$（K 的单位元），所以 e 也是商，再因为

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ba}=e,\quad a,\ b\neq 0,$$

所以 $\frac{a}{b}$ 的逆元是商 $\frac{b}{a}$，于是 F 对乘法也成群，因此 F 是体.

最后，对于 R 中任意元 a，我们有 $\frac{ab}{b}=a$，这里 b 是 R 中任意非零的元，所以 $F\supseteq R$，因此定理得证.

从上面的证明我们可以看出两件事情：第一，在我们的证明中，只要 R 能够嵌入一个体中，就可以证明 R 的商体 F 存在，并且两个商的相等以及它们的加法，乘法都完全是由 R 的结合法一意确定，所以商体 F 的构造完全是由 R 确定，因此如果 R 能够嵌入两个体中，那末所得到的两个商体就同构，也就是说，R 的商体都同构．我们更可以知道，同构的环的商体也是同构的．第二，任一体 K，如果包含 R，也就包含 R 的商体 F．因此 F 是包含 R 的最小体．譬如有理数体 Q 是整数环 Z 的商体，它是包含 Z 的最小体.

现在我们来讨论一般可换环 R（包含它的体不是已知）是否有商体？假如有，当然也是由 R 中元的商形成的可换体，但是这时商是表示什么？我们如何来认识？

我们知道体中没有零因子，如果 R 有商体 F，因为 R 是 F 的子集，所以 R 也不能有零因子，也就是说 R 必须是整环．这是必要条件，下面我们来证明它也是充分条件.

定理 2　可换环 R 有商体的必要充分条件是 R 为整环.

证明 定理的必要性已如上述，现在只证明充分性就行了.

先考虑 R 中所有元素对 (a, b)，$b\neq 0$. 两个元素对 (a, b)，(c, d)，当 $ad=bc$ 时，我们用记号

$$(a, b)\sim(c, d)$$

来表示. 显然，这个关系满足自反律、对称律，并且它也满足传递律. 这是因为，由

$$(a, b)\sim(c, d),\quad (c, d)\sim(e, f),$$

就可以得到

$$ad=bc,\quad cf=de,$$

因此

$$adf=bcf=bde.$$

但 R 是整环，所以 $af=be$，即 $(a, b)\sim(e, f)$. 于是这关系是一个等价关系，由 §1.2 定理，我们可以根据这关系把所有这些元素对形成的集分成为若干类，使相互等价的同在一类. (a, b) 所在的类用 $\frac{a}{b}$ 来表示. 下面我们来讨论由所有这些类形成的集 F.

显然，$\frac{a}{b}=\frac{c}{d}$ 的必要充分条件是 $(a, b)\sim(c, d)$，也就是 $ad=bc$. 因此，定理 1 证明中的计算法则 1°，2° 这时都同样成立.

再我们用前面的计算法则 3°，4° 来做这些类的加法、乘法的定义，也就是说，我们规定

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

这个规定是一意的. 首先因为 $b\neq 0$，$d\neq 0$，R 又没有零因子，所以 $bd\neq 0$，因此 $\frac{ad+bc}{bd}$ 及 $\frac{ac}{bd}$ 都有意义，也就是说，这两个类的确都是 F 中元. 其次，如果 $\frac{a'}{b'}=\frac{a}{b}$，$\frac{c'}{d'}=\frac{c}{d}$，我们很容易证明

$$\frac{a'd'+b'c'}{b'd'}=\frac{ad+bc}{bd},\quad \frac{a'c'}{b'd'}=\frac{ac}{bd},$$

因此 $\frac{a}{b}+\frac{c}{d}$ 及 $\frac{a}{b}\cdot\frac{c}{d}$ 的结果与在类 $\frac{a}{b}$, $\frac{c}{d}$ 中所选取的元素对 (a, b), (c, d) 没有关系，也就是说，这些类的和及积是一意的。再我们这样定义的加法及乘法显然都满足交换律，并且关于加法及乘法的结合律都是成立的．又因为

$$\left(\frac{a}{b}+\frac{c}{d}\right)\frac{e}{f}=\frac{ad+bc}{bd}\cdot\frac{e}{f}=\frac{(ad+bc)e}{bdf},$$

$$\frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}=\frac{ae}{bf}+\frac{ce}{df}=\frac{adef+bcef}{bdf^2}$$

$$=\frac{(ad+bc)ef}{bdf^2}=\frac{(ad+bc)e}{bdf},$$

所以分配律也成立．

所有元素对 $(0, a)$, $(0, b)$, $\cdots$, a, $b\neq 0$, 都属于同一类 $\frac{0}{a}$，它是加法的单位元，也就是说它是零元，这是因为

$$\frac{0}{a}+\frac{c}{d}=\frac{0d+ac}{ad}=\frac{ac}{ad}=\frac{c}{d}.$$

类 $\frac{-a}{b}$ 是 $\frac{a}{b}$ 的负元，这是因为

$$\frac{a}{b}+\frac{-a}{b}=\frac{a-a}{b}=\frac{0}{b}.$$

所有元素对 (a, a), (b, b), $\cdots$, $a, b, \cdots\neq 0$, 都属于同一类 $\frac{a}{a}$，它是乘法的单位元，这是因为

$$\frac{a}{a}\cdot\frac{c}{d}=\frac{ac}{ad}=\frac{c}{d}.$$

类 $\frac{a}{b}$ $(\neq 0)$ 的逆元是 $\frac{b}{a}$，这是因为

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ab},$$

因此我们证明了 F 成为体.

下面我们证明 R 与 F 的一个子环同构. 我们来考虑 F 中所有形状象 $\frac{aq}{q}$, $q\neq 0$, 的元的集 S. 因为 $\frac{aq}{q}=\frac{aq'}{q'}=\frac{aq''}{q''}$, 所以不妨固定一个 q, 因此 S 是所有象 $\frac{aq}{q}$, $a\in R$, 的元组成的集, 显然它是 F 的子环. 假如命 R 中元 a 与 S 中元 $\frac{aq}{q}$ 对应, 即 $a\to\frac{aq}{q}$, 那末这对应是 R 射到 S 上的可逆映射, 这是因为, 从

$$\frac{aq}{q}=\frac{bq}{q},\quad q\neq 0,$$

就得到

$$aq^2=bq^2,$$

但 R 没有零因子, 所以 $q^2\neq 0$. 因此 $a=b$. 再从

$$a\to\frac{aq}{q},\quad b\to\frac{bq}{q},$$

我们就有

$$a+b\to\frac{(a+b)q}{q}=\frac{aq+bq}{q}=\frac{aq}{q}+\frac{bq}{q},$$

$$a\cdot b\to\frac{abq}{q}=\frac{abqq}{qq}=\frac{aq\cdot bq}{q\cdot q}=\frac{aq}{q}\cdot\frac{bq}{q},$$

所以这映射是 R 射到 S 上的同构, 即 $R\cong S$. 因此 S 也是环.

根据 §3.3 定理 4, 我们可以把 R 看成 F 的一部分, 也就是说 $F\supseteq R$, 因此 F 就是 R 中所有元的商形成的体, 所以 F 是 R 的商体. 于是定理得证.

上面虽然是定理 2 的充分性的证明, 但同时也是把一个整环嵌入一个可换体的方法, 因此对任一整环我们都可以作出它的商体.

假如 R 是可换环, S 是 R 中所有非零因子的集合, 因为 ab 是零因子时, a, b 中最少有一是零因子, 所以 S 是半群. 同上面一

样，R 能够嵌入由所有商 $\frac{r}{s}$，$r\in R$，$s\in S$，形成的环中，这环叫做 R 的商环．显然它有单位元，并且 S 中任意非零元在商环中都有逆元．要注意的是，非可换无零因子环一般是没有商体的，也就是说它不能够嵌入于体．1936 年马尔采夫 (А. И. Мальцев) 曾给出了一个例子[7]来说明这个问题，但是也有有商体的，譬如非可换主理想子环环(§3.9)就有商体[8]．1931 年渥尔 (O. Ore) 曾证明[9]，一般非可换无零因子环假如满足任意两元 a,b 都有左(右)公倍元 $ab'=ba'\neq 0(b''a=a''b\neq 0)$ 的条件，它就有商体，也就是说它能够嵌入于体．这些我们都不详细证明了．

习 题 3.4

1．假设 p 是质数，试证所有形状象 $\frac{m}{n}$，$(n,p)=1$，的有理数集成为整环，并求它的商体．

2．试证任意适合消去律的可换半群能够嵌入于群．

3．假定 R 是没有单位元的环，Z 是整数环，试证所有形状象 (a,m)，$a\in R$，$m\in Z$，的元适合下列关系：

1) $(a,m)=(b,n)$，当 $a=b$，$m=n$，

2) $(a,m)+(b,n)=(a+b,m+n)$，

3) $(a,m)\cdot(b,n)=(ab+na+mb,m\cdot n)$

时，形成一个有单位元的环，单位元是 $(0,1)$，我们用 (R,Z) 表示．它包含 R 及 Z，因此，任意没有单位元的环能够嵌入一个有单位元的环，也就是说，任意没有单位元的环能够看成为有单位元的环的子环．

§3.5 多 项 式 环

我们已经知道环的一般概念，这节介绍一种特殊的环，它的结合法是具体的，并且它在数学上也占极重要地位．

普通代数中讨论的多项式，它的系数都是实数或复数，现在我们把这个概念推广到一般情形.

定义 假定 R 是有单位元 1 的环，x 是记号，也就是未定元，那末

(1) $$f(x)=\sum a_i x^i=a_0x^0+a_1x+a_2x^2+\cdots+a_nx^n,\quad a_i\in R,$$

叫做环 R 中 x 的**多项式**，或者简称为 x 的多项式，a_i 叫做它的**系数**.

首先我们规定，在 $f(x)=\sum a_i x^i$ 中，当 $a_j=0$ 时 a_jx^j 就可以略去不写，也就是说，在一个多项式中我们可以任意增加或减少系数是零的项. 再我们来规定两个多项式 $\sum a_i x^i$, $\sum b_i x^i$ 的相等以及它们的加法、乘法，这些也正是普通代数中多项式的计算法则:

(2) $$\sum a_i x^i=\sum b_i x^i,\ \text{当 } a_i=b_i,$$

(3) $$\sum a_i x^i+\sum b_i x^i=\sum(a_i+b_i)x^i,$$

(4) $$\sum a_i x^i\cdot\sum b_i x^i=\sum c_i x^i,\ c_i=\sum_{k+l=i}a_kb_l.$$

在 (2)，(3) 两式中，如果两个多项式的项数不同，我们可以用系数是零的项来填补.

由 (4) 定义的多项式乘法非常容易记忆，只要把多项式中形式的加法与乘法假定分配律成立而展开就得了. 但要注意的是 a_i, b_j 的顺序不能颠倒，因为 R 不一定是可换环.

我们很容易证明，R 中所有 x 的多项式形成一个环，叫做**由 R 添加未定元 x 形成的环**，或者叫做 **R 上 x 的多项式环**，或简称 x 的**多项式环**，用记号 $R[x]$ 来表示. 这时系数都是零的多项式是它的零元，多项式 $\sum a_i x^i$ 的负元是

$$\sum(-a_i)x^i=-\sum a_i x^i.$$

系数 $a_i\neq 0$ 的 i 中最大数，叫做多项式的**次数**. 譬如在 (1) 中，如果 $a_n\neq 0$，那末 $f(x)$ 就是 n 次，这时，a_nx^n 就叫做 $f(x)$ 的首项. 一个零次多项式是象 a_0x^0, $a_0\neq 0$, 形状的. 如果多项式的所有系数都是零，那末它就没有次数了. 因此 $R[x]$ 的零元就是没有次数的

多项式.

$R[x]$中所有零次多项式及零元形成一个子环，假如我们把 R 中元 a 与多项式 ax^0 对应，那末这对应就是 R 射到这子环上的同构，因此 R 与这子环同构．由§3.3定理4，我们可以把 R 看成 $R[x]$的子环，也就是说把 a 看成 ax^0，于是 $R[x]$的零元就是 R 的零元，零次多项式就是 R 中非零元，所以我们又可以把(1)改写成

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n.$$

再假如我们把多项式 $1x$ 写成 x，即 $1x=x$，那末 x 就是 $R[x]$中元，因此 $R[x]$是包含环 R 及未定元 x 的环，于是 ax 就是 $R[x]$中元 a, x 的乘积.

我们知道 $R[x]$是 R 的扩张环，当然 $R[x]$不具备 R 的一切性质，但它也保持 R 的某些性质．显然，R 的单位元1就是 $R[x]$的单位元，假如 R 是可换，那末 $R[x]$也是可换，此外我们还有

定理 假定 R 是整环，那末 $R[x]$也是整环.

证明 假设 $f(x)=a_0+a_1x+\cdots+a_nx^n$, $a_n\neq 0$,

$$g(x)=b_0+b_1x+\cdots+b_mx^m,\quad b_m\neq 0,$$

那末 $$f(x)g(x)=a_0b_0+\cdots+a_nb_mx^{n+m},$$

但 R 是无零因子环，所以 $a_nb_m\neq 0$，这就是说，$R[x]$没有非零的零因子，于是 $R[x]$是整环，因此定理成立.

譬如 $Z[x]$是整环，这时多项式就是普通整系数多项式.

由上面的证明，我们又可以知道，假如 R 是无零因子环，$f(x)$，$g(x)$是 $R[x]$中次数分别为 n, m 的多项式，那末 $f(x)g(x)$ 就是 $R[x]$中次数是 $n+m$ 的多项式．当 R 有零因子时，$R[x]$显然也有零因子．关于 $R[x]$的零因子，1942年麦珂(N.H. McCoy, 1905～)曾经证明了这样一个性质[10]，假定 R 是可换环，那末 $f(x)$ 是 $R[x]$的零因子的必要充分条件是，R 中有一非零元 a，使 $af(x)=0$. 1954年斯谷脱(W. R. Scott, 1919～)用反证法来证明，非常简

单，读者可参考文献[11].

现在我们来讨论未定元 x 取"值"的问题.

我们把 R 的扩张环 R' 中一元 α 来代替多项式(1)中未定元 x，就得到 $x=\alpha$ 时 $f(x)$ 的值

$$f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n,$$

它当然仍然是 R' 中一元. 假如 $f(x)=\sum a_ix^i$, $g(x)=\sum b_ix^i$, 那末它们的和及积

$$s(x)=f(x)+g(x),\quad p(x)=f(x)g(x)$$

当 $x=\alpha$ 时的值就分别是 $s(\alpha)$, $p(\alpha)$. 我们要注意的是, $s(\alpha)$ 与 $f(\alpha)+g(\alpha)$ 的意义不同，同样 $p(\alpha)$ 与 $f(\alpha)g(\alpha)$ 的意义也不同. 这是因为 $f(\alpha)$, $g(\alpha)$ 是 R' 中元，$f(x)$，$g(x)$ 是 $R'[x]$ 中元，$s(\alpha)$, $p(\alpha)$ 是先结合而后代入的结果，而 $f(\alpha)+g(\alpha)$, $f(\alpha)g(\alpha)$ 则是先代入后结合的结果，两者可能不一致. 但

$$\begin{aligned}s(\alpha)&=(a_0+b_0)+(a_1+b_1)\alpha+\cdots+(a_n+b_n)\alpha^n\\&=(a_0+a_1\alpha+\cdots+a_n\alpha^n)+(b_0+b_1\alpha+\cdots+b_n\alpha^n)\\&=f(\alpha)+g(\alpha),\end{aligned}$$

而
$$p(\alpha)=a_0b_0+(a_0b_1+a_1b_0)\alpha+\cdots+a_nb_m\alpha^{n+m}$$

却不一定与 $f(\alpha)g(\alpha)$ 相等，因为这时 α 不一定与 b_i 都能够交换. 为了避免这种困难，当我们用 R' 中元 α 来代替多项式 $f(x)$ 的未定元 x 时，我们要求 α 与 $f(x)$ 的所有系数都能够交换，这样也就有 $p(\alpha)=f(\alpha)g(\alpha)$ 了. 如果 R' 是可换环，那末 R' 中任意元都可以代入 $f(x)$ 中. 假如 $f(\alpha)=0$，那末 α 叫做 $f(x)$ 的零点，有时也叫做 $f(x)$ 的根. 以后我们说 α 是 $f(x)$ 的零点或根，就意味着 α 是 R 的扩张环中元，并且它与 R 中任意元能够交换.

下面我们来讨论关于 $R[x]$ 的欧几里得(Euclid)法式.

假定 $g(x)=b_0+b_1x+\cdots+b_{m-1}x^{m-1}+x^m$ 是 $R[x]$ 中 m 次多项式，它的首项系数是 1，又 $f(x)=a_0+a_1x+\cdots+a_nx^n$, $a_n\neq 0$, 是

$R[x]$中任一多项式，那末在 $R[x]$ 中就有两个满足

$$f(x)=q(x)g(x)+r(x) \tag{5}$$

的多项式 $q(x)$, $r(x)$, 这时 $q(x)$ 叫做 $g(x)$ 除 $f(x)$ 的**右商**, $r(x)$ 是次数小于 m 的多项式或是零元. 叫做 $g(x)$ 除 $f(x)$ 的**右余式**. 这是因为，假如 $g(x)$ 的次数大于 $f(x)$ 的次数，我们取 $q(x)=0$, $r(x)=f(x)$, 那末(5)式就显然成立. 假如 $g(x)$ 的次数不大于 $f(x)$ 的次数，我们可以自 $f(x)$ 减去 $a_n x^{n-m} g(x)$, 在所得到的多项式 $f(x)-a_n x^{n-m} g(x)=r_1(x)$ 中, x^n 的系数是零元, 所以它的次数小于 n. 如果 $r_1(x)$ 的次数大于 m, 我们可以再用同样的方法, 自 $r_1(x)$ 中减去 $g(x)$ 的倍数, 这样继续下去, 在有穷回后, 一定可以得到一个多项式 $r(x)$, 它的次数小于 m 或者是 $r(x)=0$, 因此(5)式成立.

如果 R 是体, $g(x)$ 的首项系数就可以是任意元 b_m, 而不必要求是 1, 因为对于 $\frac{1}{b_m}g(x)$, 我们有

$$f(x)=q(x)\cdot\frac{1}{b_m}g(x)+r(x)=q(x)\frac{1}{b_m}\cdot g(x)+r(x),$$

把 $q(x)\frac{1}{b_m}$ 看成(5)式中的 $q(x)$, 那末(5)式就显然成立.

同上面一样，在 $R[x]$ 中有满足

$$f(x)=g(x)q_0(x)+r_0(x) \tag{6}$$

的多项式 $q_0(x)$, $r_0(x)$, 这时 $q_0(x)$ 叫做 $g(x)$ 除 $f(x)$ 的**左商**, $r_0(x)$ 是次数小于 m 的多项式或是零元, 叫做 $g(x)$ 除 $f(x)$ 的**左余式**. 当 R 是可换时, 右商也是左商, 右余式也是左余式, 这时我们就简称为**商**及**余式**. 当 R 是无零因子环时, (5)式中的 $q(x)$, $r(x)$ 及(6)式中的 $q_0(x)$, $r_0(x)$ 都是唯一的. 上面(5), (6)两式, 我们叫做**欧几里得法式**, 或简单地叫做**欧氏法式**.

同普通代数中讨论的一样, 当 R 是可换体时, $R[x]$ 中多项式

$f(x)$, $g(x)$的最大公因式$d(x)$可以引用欧氏法式求得,并且

$$d(x)=u(x)f(x)+v(x)g(x), \quad u(x), v(x)\in R[x],$$

因此$d(x)$是$R[x]$中元.

假定α是R的扩张环中元,如果α是$R[x]$中非零的多项式的零点,那末α就叫做R的**代数元**.如果α不是$R[x]$中非零的多项式的零点,也就是说,它不适合$R[x]$中任意非零的多项式,那末α就叫做R的**超越元**.我们容易证明,$R[x]$射到$R[\alpha]$上的映射

$$\sum a_i x^i \to \sum a_i \alpha^i,$$

当α是R的代数元时,它是同态;当α是R的超越元时,它是同构.因此上面所说的未定元x是R的超越元.

我们知道$R[x]$的单位元就是R的单位元,也就是说,$R[x]$也是有单位元的环,因此我们又可以自$R[x]$再添加一个未定元y,得到环$R[x][y]$.一般,我们可以在R上陆续添加n个未定元$x_1, x_2, \cdots, x_n$,得到$R[x_1][x_2]\cdots[x_n]$.如果我们假定这些未定元能够相互交换,那末在R上添加这些元时,就与添加的顺序无关,这时就写成$R[x_1, x_2, \cdots, x_n]$,叫做由R**添加n个未定元$x_1, x_2, \cdots, x_n$的环**,或者叫做**n个未定元的多项式环**,其中的多项式可以写成

$$f(x_1, x_2, \cdots, x_n)=\sum a_{i_1 i_2\cdots i_n} x_1^{i_1} x_2^{i_2}\cdots x_n^{i_n}.$$

同一个未定元的情形一样,很容易证明,假如R是可换,那末$R[x_1, x_2, \cdots, x_n]$也是可换;假如R是整环,那末$R[x_1, x_2, \cdots, x_n]$也是整环,R或它的扩张环中与R的所有元能够交换的元可以代入$R[x_1, x_2, \cdots, x_n]$中任一多项式而得出它的值.当R是可换环时,如果$f(x_1, x_2, \cdots, x_n)$是$R[x_1, x_2, \cdots, x_n]$的零因子,那末R中也有非零的元a存在,使$af(x_1, x_2, \cdots, x_n)=0$[12].

习　题　3.5

1. $R[x]$中一个 m 次多项式与一个 n 次多项式的乘积是否是一个 $m+n$ 次多项式，为什么？

2. 假定 $f(x)$ 是 $R[x]$中多项式，a 是 R 的扩张环中元，试证"剩余定理"

$$f(x)=q(x)(x-a)+f(a).$$

3. 假定 $Z_2[x]$中多项式

$$f(x)=\begin{pmatrix}1&1\\0&1\end{pmatrix}+\begin{pmatrix}2&0\\2&0\end{pmatrix}x^2,\quad g(x)=\begin{pmatrix}1&2\\-2&1\end{pmatrix}+\begin{pmatrix}1&0\\0&1\end{pmatrix}x,$$

试求 $g(x)$除 $f(x)$的右商 $q(x)$，右余式 $r(x)$及左商 $q_0(x)$，左余式 $r_0(x)$.

4. 假定 $x_1, x_2, \cdots, x_n, \cdots$是无穷多个未定元，$R$ 是环，试定义多项式环 $R[x_1, x_2, \cdots, x_n, \cdots]$，其中多项式包含有穷个未定元.

§3.6　理　想　子　环

在 §2.5 中，我们得知由正规子群可以做商群，环可以看成加群，所以由子环可以做同余加群．但有的同余加群又能够成为环，譬如 §3.1 中给出的 $Z-(n)$ 就是环．因此我们要问，一般怎样子环的同余加群才能成为环？这种子环要满足什么条件？这样就引进了理想子环的概念.

我们知道，环 R 关于它的子环 N 的同余加群 $R-N$ 是所有同余类 $a+N=\bar{a}$ 的集合，因为当 $a\equiv a'(N)$，$b\equiv b'(N)$ 时，$a+b\equiv a'+b'(N)$，所以我们可以规定 $\bar{a}$, $\bar{b}$ 的和为 $\bar{a}+\bar{b}=\overline{a+b}$．要希望 $R-N$ 成环，首先还要规定 $\bar{a}$, $\bar{b}$ 的积．同 §3.1 中 $Z-(n)$的情形一样，我们来考虑同余类 $\bar{a}$ 中任意元与同余类 $\bar{b}$ 中任意元的乘积是否与 ab 同在一同余类．也就是说，由 $a\equiv a'(N)$，$b\equiv b'(N)$，我们能否得到 $ab\equiv a'b'(N)$．假如能够，那末对于 N 中任意元 n_1, n_2，我们有

$$(a+n_1)(b+n_2)=ab+an_2+n_1b+n_1n_2\equiv ab(N),$$

也就是

$$an_2+n_1b\equiv 0(N).$$

当 $n_1=0$ 时，$an_2\equiv 0(N)$；当 $n_2=0$ 时，$n_1b\equiv 0(N)$，因此对于 R 中任意元 r，我们有

(1)　$$rN\subseteq N,\quad Nr\subseteq N.$$

反过来，假如子环 N 具有上面性质 (1)，显然由 $a\equiv a'(N)$，$b\equiv b'(N)$，我们就得到 $ab\equiv a'b'(N)$，但是一般的子环没有上面性质，于是我们有

定义　假定 R 是环，N 是它的子环，如果对于 $a\in N$，$r\in R$，我们就有 $ra(ar)\in N$，那末 N 就叫做 R 的**左(右)理想子环**．假如 N 是 R 的左理想子环同时又是 R 的右理想子环，也就是说，当 $a\in N$，$r\in R$ 时，$ra\in N$，$ar\in N$，我们就叫 N 做 R 的**理想子环**.

显然，N 对乘法的闭合性已包含在条件(1)中，所以 R 的子集 N 成为左(右)理想子环的条件，只要它是加群，并且满足条件：当 $a\in N$，$r\in R$ 时，$ra(ar)\in N$ 就行了.

假如 R 是可换环，那末左，右理想子环及理想子环的意义是一致的，因此可换环中，理想子环就不必区别左与右的了.

于是 R 中理想子环 N 的同余类 $\bar{a}$，$\bar{b}$ 的积，我们可以规定为

$$\bar{a}\cdot\bar{b}=\overline{ab}.$$

显然 $R-N$ 对这样规定的乘法是闭合的．再因为 R 中元满足结合律、分配律，所以 N 的同余类也同样满足结合律、分配律．因此 $R-N$ 成环，这环我们叫做 R 关于 N 的**同余环**．我们容易知道，$R-N$ 的零元就是 R 的零元 0 所在的同余类 $\bar{0}$，也就是 N 自身．当 R 有单位元 e 时，e 所在的同余类 $\bar{e}$，就是 $R-N$ 的单位元．假如 R 是可换，那末同余环 $R-N$ 也是可换.

要注意的是，上面因为我们希望 N 的两个同余类的积仍然是 N 的一个同余类，所以要求 N 是理想子环，这与§2.3 中陪集

aH, bH 的积是陪集 abH 时,要求 H 是正规子群的情形一样.

上面介绍了理想子环及同余环的概念,现在我们来讨论理想子环.

显然,环自身是它的理想子环,叫做**单位理想子环**. 只一个零元也形成理想子环,叫做**零理想子环**. 由定义我们容易得知,偶数环是整数环 Z 的理想子环. 在全矩阵环 Z_2 中,所有形状象 $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ 的矩阵形成它的左理想子环而不是右理想子环. 所有形状象 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ 的矩阵形成它的右理想子环,但不是左理想子环. 所有形状象 $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ 的矩阵形成 Z_2 的子环,不是左理想子环也不是右理想子环.

下面主要是理想子环的形成.

假定 R 是可换环,a 是 R 中一元,那末 R 中所有形状象

(2) $$ra+na, \quad r\in R,\ n \text{ 是整数或零}^{*)}$$

的元形成一个理想子环,叫做由元 a **生成的理想子环**,用 (a) 表示,这是因为

$$(r_1a+n_1a)-(r_2a+n_2a)=(r_1-r_2)a+(n_1-n_2)a\in(a),$$
$$r_1(ra+na)=r_1ra+nr_1a=(r_1r+nr_1)a\in(a),$$

所以 (a) 是理想子环.

不难看出,任意包含 a 的理想子环都包含 (a),因此我们也说 (a) 是包含 a 的最小理想子环. 又因为任意多个理想子环的交集仍然是一个理想子环,所以 (a) 也是所有包含 a 的理想子环的交集.

如果 R 又有单位元 e,那末 $na=(ne)a$,于是 (2) 可以写成

---

*) n 不一定是 R 中元,所以 $ra+na$ 不能写成 $(r+n)a$,因为这时 $r+n$ 不一定有意义.

$$(r+ne)a=r'a,\quad r'\in R,$$

因此这时(a)是由a的一切倍元ra形成的. 譬如在整数环Z中, 理想子环(m)就是由m的一切倍数组成的. 要注意的是, 由a生成的理想子环(a)是R中包含a的最小理想子环, 当R没有单位元时, 所有形状象ra, $r\in R$, 的元显然也形成理想子环, 一般它不包含a, 因此它不一定是由a生成的理想子环(a). 譬如在$Z/(12)=\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$中, 由所有$\bar{r}\bar{4}$, $\bar{r}\in Z/(12)$, 形成的理想子环包含$\bar{4}$, 因此它与$(\bar{4})$一致, 但由所有$\bar{r}\bar{2}$形成的理想子环就不包含$\bar{2}$, 因此它与$(\bar{2})$不一致.

同样, 我们又可以定义由可换环R中n个元$a_1, a_2, \cdots, a_n$生成的理想子环$(a_1, a_2, \cdots, a_n)$, 它是由所有形状象

$$\sum_{i=1}^{n} r_i a_i+\sum_{i=1}^{n} n_i a_i,\quad r_i\in R,\ n_i\text{是整数或零},$$

的元形成的, $a_1, a_2, \cdots, a_n$, 叫做它的**生成元**. 如果R有单位元, 那末上式又可改写成$\sum_{i=1}^{n} r_i a_i$.

我们知道, 环R的理想子环不一定是由一个元生成的, 由一个元生成的理想子环, 叫做**主理想子环**. 零理想子环是主理想子环, 因为$0=(0)$; 单位理想子环R, 当R有单位元e时也是主理想子环, 因为$R=(e)$. 多项式环$Z[x]$中所有常数项是偶数的多项式形成的理想子环是由x, 2生成的理想子环$(x, 2)$, 它不是主理想子环.

假定R是体, $N\neq 0$是R的左理想子环, a是N中非零的元, 因为$a^{-1}a=e\in N$, 所以R中任意元$r=re\in N$, 这就是说$R\subseteq N$, 因此$N=R$. 于是体除自身及零理想子环外, 没有其他左理想子环及右理想子环.

反过来, 假如环$R\neq 0$, 除自身及零理想子环外, 它没有其他左或右理想子环, 我们命a是R中任一非零元, 因为aR是R的右

理想子环，所以$aR=R$或$aR=0$. 如果R中任意非零元a都适合$aR=R$，那末对于R中任意元b，方程$ax=b$在R中有解，因此R成体. 如果R中有某非零元a，使$aR=0$，那末对R中任意元r，我们有$ar=0$，这时显然

$$0,\ \pm a,\ \pm 2a,\ \cdots,\ \pm na,\ \cdots$$

形成R的右理想子环，因此它就是R. 于是R是循环加群. 它只有在元数是质数时才是单群，所以R是由质数p个元$0, a, \cdots, (p-1)a$形成的环. 其中任意两元的乘积都是零，于是我们有

定理 1 假如R是非零环，除自身及零理想子环外，它没有其他左或右理想子环，那末R是体或是元数为质数的幂零元环.

由上面的讨论，我们即得

定理 2 非零的有单位元的环，除自身及零理想子环外，没有其他左或右理想子环的必要充分条件是：它是体.

一个环至少有两个理想子环，一个是它自身——单位理想子环，一个是零理想子环. 只有这两个理想子环的环叫做**单纯环**，或简称**单环**. 显然体是单环. 由定理1，我们又有

定理 3 可换单环是体或是元数为质数的幂零元环.

假如N是环R的理想子环，那末N_n是全矩阵环R_n的理想子环，因此如果R是单环，那末R_n也是单环. 反过来基本上也成立，即假如R是有单位元的环，那末全矩阵环R_n的任意理想子环是全矩阵环N_n，这里N是R的理想子环[13]. 要注意的是，这里有单位元是一个不可缺少的条件. 假如R没有单位元，这定理就不成立，后面§3.6的习题2是一个明显的例.

与汉弥尔顿群类似，有汉弥尔顿环. 一个环，如果它的任意子环都是理想子环，那末这环叫做汉弥尔顿环[14]. 譬如整数环就是汉弥尔顿环.

最后我们来讨论理想子环与环的关系. 正规子群是群的重要

子群，理想子环是环的重要子环，理想子环在环中地位与正规子群在群中地位类似．下面定理更能说明这问题．这些定理及它的证法与§2.5中差不多，因此也可说是§2.5定理在环中的推广．

定理4 假定环 R 与环 R' 同态，R 中元 a 在 R' 中的象是 a'，那末 R' 的零元 $0'$ 的完全象源 N 是 R 的理想子环，叫做这同态的同态核，a' 的完全象源是同余类 $a+N$．

证明 首先，因为环的同态也是把环看成加群时的同态，所以 N 就是同态核．由§2.5定理2，我们得知 N 是加群，并且 a' 的完全象源是 N 的同余类 $a+N$．

其次，当 $a\in N$，$r\in R$ 时，我们有 $a\to 0'$，$r\to r'$，于是

$$ra\to r'0'=0', \quad ar\to 0'r'=0',$$

所以 ra，$ar\in N$，这就是说 N 是 R 的理想子环，因此定理得证．

假如两个环 R，R' 同态，即 $R\sim R'$，同态核如果是零理想子环，那末 $R\cong R'$．如果是单位理想子环，那末 R' 是零环．当 R 是单环时，因为 R 只有零理想子环及单位理想子环，所以这时同态核 $N=R$ 或者 $N=0$．因此 R' 是零环或 R 与 R' 同构，这就是说，单环的同态象是单环或是零环．假如 R，R' 都是体，因同态是 R 射到 R' 上的映射，所以这时 $N=0$，因此 $R\cong R'$．这就是§3.3中所说的体的同态是同构．

定理5 假定 N 是环 R 的理想子环，那末 R 与同余环 $R-N$ 同态，也就是说

$$R\sim R-N,$$

同态核就是 N．

证明 我们把 a 与它所在的 N 的同余类 $\bar{a}$ 对应，那末这对应显然就是 R 射到 $R-N$ 上的映射．再因为

$$a+b\to\overline{a+b}=\bar{a}+\bar{b}, \quad ab\to\overline{ab}=\bar{a}\bar{b},$$

所以 $R\sim R-N$，因此定理得证．

定理 6 假定环 R 与环 R' 同态，同态核是 N，那末

$$R-N\cong R'.$$

证明 因为 $R\sim R'$，假定这时的对应是 $a\to a'$，$\bar{a}$ 是 $R-N$ 中 a 所在的同余类 $a+N$. 由上面定理 4，我们知道 $\bar{a}$ 是 a' 的完全象源，假如我们把 $\bar{a}$ 与 a' 对应，即 $a\to a'$，显然这对应 $\bar{a}\to a'$ 是 $R-N$ 射到 R' 上的可逆映射，并且

$$\bar{a}+\bar{b}=\overline{(a+b)}\to(a+b)'=a'+b',$$

$$\bar{a}\cdot\bar{b}=\overline{ab}\to(ab)'=a'b',$$

所以 $R-N\cong R'$，因此定理成立.

于是任意同态象可以看成同余环，因此理想子环能够决定环的所有同态，这是理想子环也是同余环的一个重要性质.

同 §2.5 中一样，假如环 $R\sim R'$，N 是同态核，S 是 R 的子环，那末 S 在 R' 中的象 S' 也是 R' 的子环，并且 $S\sim S'$，同态核是 $S\cap N$，因此

$$S-(S\cap N)\cong S'.$$

当 $S\supseteq N$ 时，

$$S-N\cong S'.$$

习 题 3.6

1. 假设 R 是所有偶数形成的偶数环，试证所有形状象 $4a(a\in R)$ 的数形成一个理想子环 A，它是否是主理想子环？假如 R 是整数环 Z，A 又怎样？

2. 假定 R 是偶数环，试证所有形状象 $\begin{pmatrix}2a & b\\ c & d\end{pmatrix}$ 的矩阵，这里 a,b,c,d 都是偶数，形成全矩阵环 R_2 的理想子环.

3. 试证同态 $R\sim R'$ 是同构的必要充分条件是它的同态核 $N=0$.

4. 假定 N 是环 R 的理想子环，如果 N 是正则理想子环（即对于 N 中任意元 a，R 中有元 e_1,e_2，使 $e_1a\equiv a, ae_2\equiv a(N)$）. 那末同余环 $R-N$ 有单位元.

5. $(x,2)$ 在 $Z[x]$ 中不是主理想子环，但在 $Q[x]$ 中则是，如何证明？这里 Q 是有理数体.

6．所有形状象 $a+bi$ (a, b 是整数)的复数形成一个环，叫做**高斯数环**．试证 $Z[x]-(x^2+1)$ 与高斯数环同构，这里 Z 是整数环．

7．假定 S 是环 R 的子环，N 是 R 的理想子环，并且 $S\cap N=0$，试证同余环 $R-N$ 中有与 S 同构的子环．

8．假定 Z 是整数环，p 是质数，试证 $Z-(p^n)$ 中任意非零的理想子环包含 $\overline{p}^{n-1}$，也就是说，$Z-(p^n)$ 中所有非零理想子环的交异于零．

9．假定 R 是元数大于 1 的整环，并且只包含有穷个理想子环，那末 R 是体．

10．试证单环有单位元时中心是体，没有单位元时，中心是零．

§3.7　理想子环的运算

上节我们介绍了理想子环及它的特性，这节我们来介绍它的运算，和，积及商．

假定 A, B 是环 R 的理想子环，那末所有形状象 $a+b$, $a\in A$, $b\in B$ 的元的集，也就是它们的和 (A, B) (§2.3)，是 R 的理想子环，叫做理想子环 A, B 的和．显然，

$$(A, B)=(B, A),$$

并且

$$((A, B), C)=(A, (B, C))=(A, B, C).$$

同和的情形不一样，所有形状象

$$ab, \quad a\in A, \ b\in B$$

的元的集不能形成为 R 的理想子环，譬如 $A=(x, y)$, $B=(x^2, y)$ 是多项式环 $Z[x, y]$ 的理想子环，x^3, y^2 是形状象 ab 的元，但 x^3-y^2 就不能写成 ab 的形状．因此我们来考虑所有有穷个元 ab 的和

$$\sum a_ib_i, \quad a_i\in A, \ b_i\in B$$

的集合，这时因为

$$\sum a_ib_i-\sum a_i'b_i'=\sum a_ib_i+\sum(-a_i')b_i',$$

$$r\sum a_ib_i=\sum(ra_i)b_i,$$

所以这个集成为 R 的理想子环，叫做 A, B 的积，用 AB 来表示.

譬如在整数环 Z 中，如果 $A=(12)$, $B=(21)$，那末 $(A, B)=(3)$, $AB=(252)$.

当 $A=(a)$, $B=(b)$ 时，显然 $(A, B)=(a, b)$, $AB=(ab)$. 一般，假如 $A=(a_1, \cdots, a_m)$, $B=(b_1, \cdots, b_n)$，那末

$$(A, B)=(a_1, \cdots, a_m, b_1, \cdots, b_n),$$

$$AB=(a_1b_1, \cdots, a_1b_n, \cdots, a_mb_n).$$

这就是说，如果 A, B 是分别由 a_i, b_j, $i=1, \cdots, m$; $j=1, \cdots, n$, 生成的理想子环，那末 (A, B) 是由 a_i, b_j 生成的理想子环，AB 是由 a_ib_j 生成的理想子环.

显然，$RA\subseteq A$, $AR\subseteq A$，如果 R 有单位元，那末 $A\subseteq RA$, $A\subseteq AR$，于是 $RA=AR=A$. 因此 R 是理想子环的乘法单位，这也就是 R 所以叫做单位理想子环的一原因.

同普通乘积的意义一样，R 的理想子环 A 的 n 乘幂 A^n 的意义是用下式来规定：

$$A^1=A, \quad A^{n+1}=AA^n, \quad n \text{ 是正整数}.$$

为了方便，我们又常常把 A^0 写成 R 即 $A^0=R$. 当 $A^2=A$ 时，A 叫做**幂等理想子环**. 当 $A^n=0$ 时，A 叫做**幂零理想子环**. 这时 A 中任意 n 个元的乘积都是 0，因此任意元都是幂零元. 任意元都是幂零元的理想子环，叫做**幂零元理想子环**. 所以幂零理想子环是幂零元理想子环，但反过来不一定成立.

我们容易知道，§3.1 定理 1 中可换环的理想子环是幂零元理想子环，但不一定是幂零理想子环.

由定义，我们容易知道

$$(AB)C=A(BC),$$

即对乘法，理想子环的结合律成立. 再因为 $A(B, C)$ 中任意元

$$\sum a_i(b_i+c_i)=\sum a_ib_i+\sum a_ic_i$$

在 (AB, AC) 中；反过来，(AB, AC) 中任意元

$$\sum a_i b_i + \sum a_j c_j = \sum a_i (b_i + 0) + \sum a_j (0 + c_j)$$

又在 $A(B, C)$ 中，所以

$$A(B, C) = (AB, AC).$$

假如 R 是可换环，那末

$$AB = BA,$$

这就是说，在可换环中，理想子环对乘法的交换律成立．但消去律不成立，即由 $AB=AC$，不一定有 $B=C$．譬如在由所有形状象 $a+3b\sqrt{-5}$（a, b 是整数或零）的数形成的环中，$A=(3, 3\sqrt{-5})$；$B=(3)$，显然 $A\neq B$，但

$$A^2 = (9, 9\sqrt{-5}, -45) = (3, 3\sqrt{-5})(3) = AB.$$

我们知道在整数环 Z 中，如果 $a\in(b)$，那末 $a\equiv 0(b)$，也就是 $a=rb$，即 a 能够被 b 整除．现在我们把这概念来推广．

假定 B 是 R 的理想子环，如果 $a\in B$，即 $a\equiv 0(B)$，我们就说 a 能够被理想子环 B **整除**．当理想子环 A 中任意元能够被 B 整除，即 $A\subseteq B$，也就是 $A\equiv 0(B)$ 时，我们就说 A 能够被 B **整除**，这时 B 叫做 A 的**约理想子环**，A 叫做 B 的**倍理想子环**．要注意的是，在整数中约数不能大于倍数，但在环中，约理想子环是包含倍理想子环的．假如我们把约理解为包含，倍理解为被包含，那末约理想子环与倍理想子环的关系就容易认识而不致混淆不清了．

环 R 中任意理想子环都包含零理想子环，因此零理想子环是任意理想子环的倍理想子环．单位理想子环 R 包含任意理想子环，因此 R 是任一理想子环的约理想子环，即 R 能整除任意理想子环．在整数中，-1, 1 能够整除任意整数，在这点上，R 与 $-1, 1$ 非常类似，这是我们叫 R 做单位理想子环的另一原因．

显然，R 的理想子环 A, B 的和 (A, B) 是 A, B 的约理想子环，因此 (A, B) 是 A, B 的**公约理想子环**．但是 A, B 的任一公约

理想子环都是(A, B)的约理想子环，所以(A, B)是A, B的**最大公约理想子环**.

假如环R有单位元，如果$(A, B)=R$，那末A, B除R外没有公约理想子环，因此我们叫A、B做**互质**．这时R中任意元可以写成A, B中元的和．譬如在整数环中，由两个互质的数生成的两个理想子环是互质的．任意整数也可写成这两个质数的倍数的和．

同样，我们知道$A\cap B$是A, B的公倍理想子环，并且A, B的公倍理想子环都是$A\cap B$的倍理想子环，所以$A\cap B$是A, B的**最小公倍理想子环**.

再因为$AB\subseteq A$，$AB\subseteq B$，所以$AB\subseteq A\cap B$，这就是说，A, B的乘积AB是它们的最小公倍理想子环的倍理想子环．

我们容易知道，两个整数的最小公倍与最大公约的乘积等于这两个整数的乘积，因此在整数环中，理想子环A, B的最小公倍$A\cap B$与它们的最大公约(A, B)的乘积等于它们的乘积AB，即$(A\cap B)(A, B)=AB$，但在一般可换环中，我们只能有

$$(A\cap B)(A, B)\subseteq AB,$$

这是因为

$$\begin{aligned}(A\cap B)(A, B)&=((A\cap B)A, (A\cap B)B)\subseteq(BA, AB)\\&=AB.\end{aligned}$$

当A, B是互质的理想子环，即$(A, B)=R$时，那末$AB=A\cap B$，也就是说，这时A, B的乘积就是它们的最小公倍理想子环．

下面我们来介绍在一般可换环中理想子环商的概念．

假定A, B是可换环R的理想子环，那末R中所有适合

$$rB\equiv 0(A)$$

的元r形成R的理想子环，叫做A, B的**商**[15]，用记号$A:B$来表示．这是因为，如果r_1, r_2适合上式，显然r_1-r_2以及r_1r_2也都适

合上式，这里 r 是 R 中任意元.

由定义我们容易知道

$$A\subseteq A:B,\quad (A:B)B\subseteq A.$$

再

$$(A:B):C=(A:C):B=A:BC,$$
$$A:(B,\ C)=(A:B)\cap(A:C).$$

此外我们又有

$$(A_1\cap\cdots\cap A_n):B=(A_1:B)\cap\cdots\cap(A_n:B),$$

即 $$(\cap A_i):B=\cap(A_i:B),\quad i=1,\ \cdots,\ n,$$

这是因为由 $rB\subseteq\cap A_i$，就有 $rB\subseteq A_i$，$i=1,\ \cdots,\ n$，反过来也成立.

在整数环中，(a)，$(b)\neq 0$ 的商 $(a):(b)$ 可以这样来求得，先把 a 分解因子，再删去其中能够整除 b 的因子，剩下的数如果是 c，那末 $(a):(b)=(c)$，譬如

$$(12):(3)=(4),\ (12):(21)=(4),\ (12):(5)=(12).$$

又因为这时 c 就是 a，b 的最大公约数 $(a,\ b)$ 除 a 得到的商，所以我们又有 $(a):(b)=(a):(a,\ b)$. 这性质在一般可换环中也能够成立，即

$$A:B=A:(A,\ B).$$

这是因为

$$A:(A,\ B)=(A:A)\cap(A:B)=R\cap(A:B)=A:B.$$

我们知道 $A\subseteq A:B\subseteq R$. 当 $B\subseteq A$ 时，R 中任意元 r 都适合 $rb\equiv 0(B)\equiv 0(A)$，因此这时 $A:B=R$.

当 A，B 是互质理想子环时，我们有

$$A:B=A,\ B:A=B.$$

这是因为，假定 $A:B=C$，那末 $CB\subseteq A$，因此 $(CB,\ A)=A$. 再因为 $(A,\ B)=R$，所以

$$(C,\ A)=(C,\ A)(A,\ B)=(CA,\ A^2,\ CB,\ AB)$$
$$\subseteq (CB,\ A)=A,$$

于是 $C\subseteq A$，即 $A:B\subseteq A$，所以 $A:B=A$. 同样，我们可以证明 $B:A=B$.

要注意的是，上面这性质的逆是不成立的. 譬如在多项式环 $Z[x,\ y]$ 中，$(x):(y)=(x)$，$(y):(x)=(y)$，但 $(x,\ y)\neq(1)$.

假如 R 是非可换环，A、B 是 R 的理想子环，那末 R 中所有适合

$$rB\equiv 0(A)\quad (Br\equiv 0(A))$$

的元 r 形成 R 的理想子环，叫做 A,B 的右(左)商，用记号 $(A:B)_R$ ($(A:B)_L$) 表示. 同上面一样，我们容易得知

$$A\subseteq (A:B)_R,\ (A:B)_R\cdot B\subseteq A,$$
$$((A:B)_R:C)_R=(A:BC)_R,$$
$$(A:(B,\ C))_R=(A:B)_R\cap(A:C)_R.$$

读者试根据定义加以验证.

习　题　3.7

1. 求下列各商:

$$(6):(3),\ (6):(5),\ (3):(9).$$

2. 假定 A,B,C 是环 R 的理想子环，$B\supseteq C$，试证

$$C:A\subseteq B:A,\quad A:B\subseteq A:C.$$

3. 试证下面三个关系假如有一个成立，那末其余两个也都成立:
(i) $A:B=A$, $A:C=A$, (ii) $A:(B\cap C)=A$, (iii) $A:BC=A$.

4. 假设 a,b 是整数，d 是 a,b 的最大公约，m 是 a,b 的最小公倍，即 $d=(a,\ b)$，$m=[a,\ b]$. $A=(a)$，$B=(b)$ 是整数环 Z 的理想子环，试证:

$$(a,\ b)=(d),\quad A\cap B=(m).$$

5. 假如 B、C 都与 A 互质，那末 BC 及 $B\cap C$ 都与 A 互质.

6. 假定 $A_1,\ A_2,\ \cdots,\ A_n$ 是环 R 中两两互质的 n 个理想子环，试证

$$A_1A_2\cdots A_n=A_1\cap A_2\cap\cdots\cap A_n.$$

§3.8 极大理想子环，质理想子环

这节我们主要是介绍两个特殊的理想子环，它们在研究环时都占重要地位.

我们知道，环的任一理想子环在环中至少有两个理想子环是它的包含集，一个就是它自身，一个是单位理想子环. 一般，除这两个理想子环外，可能还有其他包含它的理想子环.

定义 1 假定 N 是 R 的理想子环，如果 R 中除 N 自身及单位理想子环 R 外，不再有其他包含 N 的理想子环，那末 N 就叫做 **R 的极大理想子环.**

因此极大理想子环除自身及单位理想子环是它的约理想子环外，不再有其他约理想子环，所以我们又叫极大理想子环做**无因子理想子环.**

单位理想子环显然是极大理想子环. 在整数环 Z 中，由质数 p 生成的主理想子环 (p) 也是极大理想子环. 这是因为，假如理想子环 $N\supset(p)$，那就有一整数 $a\in N$，但 $\overline{\in}(p)$，也就是说，N 中有不是 p 的倍数的数 a，因此 a，p 互质. 于是有两整数 r，s 存在，使 $ra+sp=1$，但 $ra\in N$、$sp\in(p)$，因此 $1\in N$，所以 $N=Z$，这就是说 (p) 除了自身外，只有单位理想子环是它的包含集，所以它是极大理想子环.

由 §3.2，我们还知道 $Z-(p)$ 是体，也就是说，整数环 Z 关于极大理想子环 (p) 的同余环 $Z-(p)$ 是体. 反过来，假如 $Z-(p)$ 是体，那末 p 是质数，于是 (p) 是极大理想子环. 因此 (p) 是 Z 的极大理想子环的必要充分条件是 $Z-(p)$ 是体. 一般在可换环中，这性质也能够成立，即

定理 1 有单位元可换环 R 的理想子环 $N(\neq R)$ 是极大理想

子环的必要充分条件是：同余环 $R-N$ 成为体.

证明 假如 N 是极大理想子环，由 §2.1 定理 2，我们只要证明对于 $R-N$ 中任意元 $\bar{a}\neq 0$, $\bar{b}$，方程

$$\bar{a}\bar{x}=\bar{b}$$

在同余环 $R-N$ 中有解，那末 $R-N$ 就是体了．因为 $\bar{a}\bar{x}=\bar{b}$ 可以写成 $ax\equiv b(N)$，所以我们就有 $b=ax+n$，因此只要能够把 b 写成 $b=ar+n$, $r\in R$, $n\in N$ 就行了．我们知道 $ar+n\in((a),N)$，因为 $a\in(a)$，而 $a\bar{\in}N$，所以 $N\subset((a),N)$，但 N 是极大理想子环，所以 $((a),N)=R$．因为 R 有单位元，所以 $((a),N)$ 中任意元可以写成 $ar+n$，也就是说，R 中任意元可以写成 $ar+n$，即 $b=ar+n$，因此 $\bar{b}=\overline{ar}=\bar{a}\bar{r}$．于是 $R-N$ 是体，所以条件的必要性成立.

再假定 $R-N$ 是体．如果理想子环 $A\supset N$，我们只要证明 $A=R$，也就是说，只要证明 R 中任意元 $b\in A$ 就行了．假定 $a\in A$，但 $\bar{\in}N$，因为 $R-N$ 是体，所以方程

$$\bar{a}\bar{x}=\bar{b}$$

在 $R-N$ 中有解，于是同余式 $ax\equiv b(N)$ 在 R 中有解，因此 $ax=b+n$．但 $ax\in A$, $n\in A$，所以 $b\equiv 0(A)$，这就是说，R 中任意元 b 都在 A 中，因此 $A=R$．所以条件的充分性成立，因此定理得证.

上面的定理虽然是理想子环 N 是极大的必要充分条件，但同时也是同余环 $R-N$ 成体的必要充分条件．要注意的是，这时 R 有单位元，假如 R 没有单位元，上定理的充分条件也能成立，但必要条件就不一定能够成立了．譬如在所有偶数形成的偶数环 S 中，(4) 是极大理想子环，这是因为，假如 $(4)\subset N$, $a\in N$，但 $\bar{\in}(4)$，那末 4, a 的最大公约数是 2，因此 $2=4r+sa$，这里 r, s 是整数．于是 $2\in N$，所以 $N=S$．这就是说 (4) 除自身及 S 外，没有其他约理想子环，因此 (4) 是极大理想子环．但 $2^2\equiv 0(4)$, $2\not\equiv 0(4)$，所以 $S-(4)$ 中有幂零元，因此它不成为体.

假如 R 是一般非可换环，上定理中充分条件也能够成立，但必要条件就不再成立了.

下面我们再来介绍可换环的另一个重要理想子环.

我们知道在整数环中，质数除自身及 1（包括正、负）外，不再有其他约数，在这点上，极大理想子环与质数类似. 再两个整数的积，如果能够用一个质数整除，那末这两个整数中至少有一个能够用这质数整除，这是质数的一个基本性质. 极大理想子环不一定都有这类似性质，但是环中有的理想子环确具有这性质.

定义 2　可换环 R 的理想子环 P，当 R 中两元 a, b 的积 ab 在 P 中时，a, b 中至少有一元在 P 中，也就是说当 $ab\equiv 0(P)$ 时，

$$a\equiv 0(P) \text{ 或 } b\equiv 0(P),$$

那末 P 叫做 R 的**质理想子环**.

单位理想子环 R 是质理想子环，因为对于 R 中任意元 a，这时都有 $a\equiv 0(R)$. 前面 Z 的主理想子环 (p) 也是质理想子环. 这是因为，如果 $ab\equiv 0(p)$，那末 $ab=mp$，因此 a, b 中必有一数能够用 p 整除，即 $a\equiv 0(p)$ 或 $b\equiv 0(p)$.

显然，可换环 R 的任一质理想子环包含 R 中所有的幂零元，但 R 中所有幂零元形成的理想子环不一定是质理想子环. 譬如 $Z-(8)$ 中所有幂零元$\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$形成质理想子环，但 $Z-(6)$ 中只有零元是幂零元，这时零子环不是质理想子环.

假如 R 是整环，那末零子环是质理想子环. 这是因为当 $ab=0$ 时，a, b 中必有一为 0，即 $a=0$ 或 $b=0$. 反过来，假如可换环 R 的零子环是质理想子环，那末 R 是整环，因此，零子环是质理想子环的必要充分条件是 R 为整环. 一般，我们有

定理 2　可换环 R 中理想子环 P 是质理想子环的必要充分条件是：同余环 $R-P$ 为整环.

证明　假如 P 是质理想子环，因为 P 是理想子环，所以 $R-P$

成环，再由 $\bar{a}\bar{b}=\bar{0}$，我们就得到 $ab\equiv 0(P)$，因此

$$a\equiv 0(P) \quad 或 \quad b\equiv 0(P),$$

于是 $\bar{a}=\bar{0}$ 或 $\bar{b}=\bar{0}$，所以 $R-P$ 是无零因子环，因此它是整环.

反过来，假如 $R-P$ 是整环，由 $ab\equiv 0(P)$，我们就得到

$$\bar{a}\bar{b}=\bar{0},$$

于是 $\bar{a}=\bar{0}$ 或 $\bar{b}=0$，因此 $a\equiv 0(P)$ 或 $b\equiv 0(P)$ 所以 P 是质理想子环，于是定理得证.

要注意的是，在有单位元的可换环中，极大理想子环是质理想子环，但它的逆不成立，即质理想子环不一定都是极大的. 譬如在整数环 Z 中，零理想子环是质理想子环，显然它不是极大理想子环. 又如在多项式环 $Z[x]$ 中，(x) 是质理想子环，但 $(x)\subset(2, x)\subset Z[x]$，因此它也不是极大理想子环.

再在没有单位元的可换环中，极大理想子环不一定是质理想子环. 譬如前面的(4)就是 S 的极大理想子环，但不是质理想子环.

上面所说的环是可换环，关于一般环，极大理想子环的概念仍如定义 1. 这时定理 1 中充分条件也成立，即假如 $R-N$ 是体，那末 N 是极大理想子环.

关于质理想子环，1949 年麦珂给出如下定义.

定义 3 假如 P 是 R 的理想子环，对 R 中任两个理想子环 A, B，如果它们的积 $AB\equiv 0(P)$ 时，我们就有 $A\equiv 0(P)$ 或 $B\equiv 0(P)$，那末 P 叫做**质理想子环**.

当 R 是可换环时，如果 P 是质理想子环，从 $ab\equiv 0(P)$，我们就有 $(a)(b)\equiv 0(P)$，所以 $(a)\equiv 0$ 或 $(b)\equiv 0$. 因此 $a\equiv 0(P)$ 或 $b\equiv 0(P)$，这就是说，定义 2 是这定义的特例.

1956 年生兹(A. D. Sands)证明了这样的定理: 假定 P 是环 R 的质理想子环，那末 P_n 是全矩阵环 R_n 的质理想子环. 反过来，R_n 的质理想子环是 P_n，这里 P 是 R 的质理想子环. 再假如 N 是

R 的极大理想子环，如果 N 又是 R 的质理想子环，那末 N_n 是 R_n 的极大理想子环[18].

一个环如果它的零子环是质理想子环，麦珂叫它做质环，因此可换质环是整环[17]．再假定 R 是有单位元的环，全矩阵环 R_n 是质环的必要充分条件是 R 是质环[18].

假如 P 是环 R 的质理想子环．显然 $R-P$ 是质环．此外，环 R 是质环的必要充分条件是：如果 $L_1L_2=0$，那末 $L_1=0$ 或 $L_2=0$，这里 L_1，L_2 是 R 的左理想子环．再 R 是质环的必要充分条件是：左零化 R 的左理想子环的左理想子环是零理想子环．这些都是质环的基本性质[19]．质环是一类重要的环，很多环的构造可以由它来决定，只是目前质环本身的构造还不清楚.

习 题 3.8

1．假设 Q 为有理数体，那末 $Q[x]$ 中 (x) 是否是极大子理想子环？

2．试证 (x)，$(2, x)$ 都是 $Z[x]$ 的质理想子环.

3．在高斯数环中，理想子环 (3)，$(1+i)$ 是否都是质理想子环？

4．假设 P 是环 R 的理想子环，Q 是 R 中所有不在 P 中的元的集合，试证 P 是质理想子环的必要充分条件是 Q 对于乘法成半群.

5．假定 A 是环 R 的理想子环，P 是环 A 的质理想子环，并且 $P\neq A$，试证 P 是 R 的理想子环.

6．假设环 $R=R^2$，试证 R 的极大理想子环也是它的质理想子环.

7．假定 N 是环 R 的理想子环，试证 $R-N$ 成体的必要充分条件是

(1) N 是极大理想子环，(2) 如果 $x^2\equiv 0(N)$，那末 $x\equiv 0(N)$.

8．环 R 的理想子环 N 是极大理想子环的必要充分条件是同余环 $R-N$ 是单环.

§ 3.9 主理想子环环中元素的因子分解

在整数环中，任意整数除因子的顺序外，可以一意分解为质因

子的乘积,也就是说质因子分解是一意的.这是一个重要定理. 我们要问在任意环中, 这定理能否成立? 现在我们只在可换主理想子环环中来讨论这问题,这问题假如在主理想子环环中解决了,那末它也就基本上解决了.

定义 1 有单位元的整环, 如果其中任意理想子环都是主理想子环,就叫做**主理想子环环**.

我们先给出下面一些重要的主理想子环环.

定理 1 整数环 Z 是主理想子环环.

证明 因为整数环 Z 是有单位元的整环, 我们只要证明其中任一理想子环 N 是主理想子环就行了.

假如 $N=0$, 显然它是主理想子环. 假如 $N\neq 0$, 那末它就含有一整数 $c\neq 0$,因此它也含有整数 $-c$, 所以 N 含有正整数. 现在假定 N 中所含的最小正整数是 a, 如果我们能够证明 N 中任意数 b 都是 a 的倍数, 即 $b=qa$, 那末 $N=(a)$, 因此 N 就是主理想子环了.

假定 b 用 a 除,我们就有

$$b=qa+r,\quad 0\leqslant r<a,$$

因为 $b\in N$, $a\in N$,所以

$$r=b-qa\in N.$$

但 a 是 N 中最小正整数,所以 $r=0$,因此 $b=qa$, 于是定理得证.

多项式环 $Z[x]$ 虽然也是有单位元的整环,但由 §3.6, 我们得知它的理想子环不都是主理想子环,因此它不是主理想子环环.

定理 2 假定 F 是可换体,那末多项式环 $F[x]$ 是主理想子环环.

证明 首先,因为 F 的单位元 1 也是 $F[x]$ 的单位元, 又因 F 是可换体, 由 §3.5 定理, $F[x]$ 是整环, 因此 $F[x]$ 是有单位元的整环.

再，假定 $N\neq 0$ 是 $F[x]$ 的理想子环，$g(x)$ 是 N 中次数最低的一个多项式，那末 N 中任一多项式 $f(x)$ 我们可以引用欧氏法式把它写成

$$f(x)=q(x)g(x)+r(x),$$

这里 $r(x)$ 是零元或者它的次数小于 $g(x)$ 的次数．同上面定理的证明一样，我们有 $r(x)=0$，所以 N 是主理想子环，因此定理得证．

下面我们再给出一类重要的主理想子环环．

假定 R 是整环，如果对于其中任意非零的元 a，有整数 $\sigma(a)\geqslant 0$，并且对于 R 中任意元 $a\neq 0$，b，在 R 中有适合欧氏法式

$$b=qa+r,\quad a\neq 0$$

的元 q，r，这里 $r=0$ 或 $\sigma(r)<\sigma(a)$，那末 R 叫做**欧几里得环**，或简称为**欧氏环**．

显然，整数环 Z 是欧氏环，因为我们可以取 $\sigma(a)=|a|$；此外，多项式环 $F[x]$ 也是欧氏环，因为我们可以取 $\sigma(f(x))=f(x)$ 的次数．

定理 3 欧氏环是主理想子环环．

证明 假定 $N\neq 0$ 是欧氏环 R 的理想子环，a 是 N 中 $\sigma(a)$ 最小的一元．同定理 1 的证明一样，引用欧氏法式我们很容易知道 N 中任意元 b 是 a 的倍元，即 $b=qa$，因此 $N=(a)$，这就是说，R 中任意理想子环都是主理想子环．再我们命 $R=(r)$，由上面的证明，我们得知 R 中任意元可以写成 qr，因此 r 自身也是如此．假如 $r=er$，那末对于 R 中任意元 $s=qr$，我们有 $es=eqr=s$，于是 e 是 R 的单位元．这就是说 R 是有单位元的整环，所以 R 是主理想子环环，因此定理得证．

要注意的是这定理的逆是不成立的，也就是说，主理想子环环不一定是欧氏环．1949 年马士肯 (T. S. Matzkin) 曾给了一个例

来说明这问题，读者可参考原始资料[20].

现在我们来讨论因子分解问题．首先我们规定几个基本概念．它们都与整数环中的类似．

假定 R 是有单位元 e 的整环，其中有的元有逆元，有的元没有逆元，可逆元是有逆元的元．元 a 如果可以写成

$$a=r_1r_2\cdots r_n,\quad r_i\in R,$$

就叫做 a 的**因子分解**，r_i 叫做 a 的因子，也叫做 a 的**约元**，a 又叫做 r_i 的**倍元**．这时我们又说 a 可以用 r_i **整除**．显然，a 可以写成

$$a=ae=(-a)(-e)=a(-e)(-e)$$

等等，更一般地，如果 c 是 R 中可逆元，它的逆元是 c^{-1}，我们又有

$$a=a\cdot cc^{-1}=ac^{-1}\cdot c.$$

象这样含有可逆元做因子的因子分解，我们叫它做**显然的分解**．同在整数环中一样，这样的分解我们不讨论．下面讨论的是 r_i 都不是可逆元的非显然分解．

假如 a 是 b 的约元，同时 b 又是 a 的约元，即 $b=ma$，$a=nb$，那末 $b=mnb$．因为 R 是整环，所以 $mn=e$，这就是说 m，n 都是可逆元．因此 a，b 相差只是一个可逆元的因子．反过来，假如 $a=bc$，c 是可逆元，那末 $b=ac^{-1}$，因此 a 又是 b 的约元．我们把相差只是一个可逆元因子的两个元叫做**相伴**．于是 a，b 相伴的必要充分条件是 a，b 互为约元．与 e 相伴的元是可逆元．

我们知道，任意与 a 相伴的元都是 a 的约元，任意可逆元也都是 a 的约元．假如 b 是 a 的约元，而 b 不是可逆元，又不与 a 相伴，那末 b 就叫做 a 的**真约元**．

同质数类似，我们有下面质元的概念．

定义 2 在有单位元的整环 R 中，元 $a\neq0$，并且不是可逆元，如果它有真约元，就叫做**可分解元**；如果它没有真约元，就叫做**不可分解元**，或叫做**质元**．多项式环中的质元又叫做**既约多项式**．

于是,假如 p 是 R 的质元,由 $p=ab$,我们就得知 a, b 中有一是可逆元. 假如 q 是 R 的可分解元,那末在 R 中有不是可逆元 a, b 存在,使 $q=ab$. 又我们容易证明,质元与可逆元的乘积还是质元,也就是说,与质元相伴的元还是质元.

我们知道,在证明整数的因子分解时,要引用整数的大小顺序关系,但在主理想子环环中元没有顺序关系,下面的定理就是用来代替这关系的.

定理 4 假定 $a_1, a_2, \cdots, a_n, \cdots$ 是主理想子环环 R 中元,并且任意 a_{i+1} 能够整除 a_i,那就有一个整数 m 存在,当 $i\geqslant m$ 时,所有的 a_i 都彼此相伴.

证明 假定 R 中各个 a_i 的所有倍元 ra_i, $r\in R$,的集合是 N, b, c 是 N 中任意元,那末

$$b=ra_i, \quad c=sa_j, \quad i\geqslant j.$$

但 a_j 可以用 a_i 整除,也就是说 $a_j=ta_i$,因此

$$b-c=ra_i-sta_i=(r-st)a_i\in N,$$

所以 N 是 R 的理想子环. 假定 $N=(d)$, $d=ra_m$, 那末任意 $a_i=kd=kra_m$,即 a_m 是任意 a_i 的约元,但当 $i\geqslant m$ 时,a_i 又是 a_m 的约元,因此这时 a_i 与 a_m 相伴,这就是说,当 $i\geqslant m$ 时,所有的 a_i 都彼此相伴,因此定理成立.

现在我们来讨论主理想子环环中元的分解.

我们容易知道,零元不能分解为有穷个质元的乘积,这是因为,假如

$$0=r_1r_2\cdots r_n,$$

那末其中某个 $r_i=0$,但零元不是质元. 同样,可逆元也不能分解为有穷个质元的乘积,因为如果

$$a=r_1r_2\cdots r_n,$$

那末

$$e=r_1(a^{-1}r_2\cdots r_n),$$

因此 r_1 是可逆元，但可逆元不是质元.

定理 5 主理想子环环 R 中任意不是零元又不是可逆元的元，能够分解为有穷个质元的乘积.

证明 我们用反证法来证明. 假如定理不成立，a 是不满足定理的一元，也就是说，a 不能够分解为有穷个质元的乘积. 显然 a 不是质元，所以

$$a=bc,$$

这里 b, c 都不是可逆元，因此 b, c 都不与 a 相伴，并且 b, c 中最少有一元也不能够分解为有穷个质元的乘积. 令这元是 $b=a_1$. 再引用上面的方法就得到能够整除 a_1 但又不与 a_1 相伴的元 a_2，这样继续推求，我们就有

$$a, a_1, a_2, \cdots, a_n, \cdots,$$

这里 a_{i+1} 能够整除 a_i，但 a_i 与 a_i 不相伴，这与上面定理 4 矛盾，因此定理成立.

在整数环中，证明因子分解的一意性时要引用质数的一个基本性质：两整数的乘积如果能够用一个质数整除，那末这两个整数中至少有一数能用这质数整除. 现在我们要问，在主理想子环环中，质元是否也有这基本性质？我们知道，假如质元 p 有这性质，那末 (p) 就是质理想子环. 反过来，假如 (p) 是质理想子环，那末质元 p 就有这性质. 但是在主理想子环环中，极大理想子环是质理想子环，因此如果能够证明 (p) 是极大理想子环，那末 p 就有这性质了.

定理 6 在主理想子环环 R 中，质元 p 生成的理想子环 (p) 是极大理想子环.

证明 假定 $(p)\subseteq(q)$，那就有 $p=rq$，因此 r, q 中必有一是可逆元. 如果 r 是可逆元，那末 $q=r^{-1}p$，所以 $(q)=(p)$. 如果 q 是

可逆元，那末 $qq^{-1}=e\in(q)$，所以 $(q)=R$. 这就是说，只有 (p) 自身及单位理想子环是 (p) 的约理想子环，因此 (p) 是极大理想子环，所以定理得证.

于是在主理想子环环中，两个元 a, b 的积 ab 如果能够用质元 p 整除，那末 a, b 中至少有一元能够用 p 整除.

再在主理想子环环中，可分解元 $q=ab$，这里 a, b 都不是可逆元，生成的理想子环 (q) 不是质理想子环，这是因为由 $ab\equiv 0(q)$，如果 $a\equiv 0(q)$，那末 $a=a'q$. 于是 $q=a'bq$，因此 $a'b=e$，这与 b 不是可逆元的假设不合.

于是在主理想子环环中，质元生成的理想子环是质理想子环，可分解元生成的理想子环不是质理想子环，非零的质理想子环是极大理想子环.

下面我们来证明质因子分解的一意性. 所谓元 a 的因子分解是一意的，就是说，如果 a 有两种因子分解

$$a=r_1r_2\cdots r_m=r'_1r'_2\cdots r'_n,$$

那末 $m=n$，并且每个 r_i 分别与某个 r'_i 相伴.

定理 7 主理想子环环 R 中任意不是零元又不是可逆元的元，除因子顺序及可逆元因子外，能够一意分解为有穷个质元的乘积.

证明 假定元 $a\neq 0$，又不是可逆元，由定理 5，a 可以分解为 m 个质元 p_i 的乘积，即 $a=p_1p_2\cdots p_m$. 如果它又可以分解为 n 个质元 q_i 的乘积，即 $a=q_1q_2\cdots q_n$，那末

$$p_1p_2\cdots p_m=q_1q_2\cdots q_n.$$

现在我们对于 m 用归纳法来证明这两种分解是一致的. 假如 $m=1$，因为这时 $a=p_1$ 是质元，但 q_i 都不是可逆元，于是 $n=1$，因此 $p_1=q_1$，所以这时定理成立. 假定对于 $m-1$ 定理成立，我们来证明对于 m 定理也能够成立. 因为 p_1 能够整除 a，也就是说能够整

除 $q_1q_2\cdots q_n$，所以 p_1 必定能够整除某一个 q_i. 我们适当的改变 q_i 的顺序，使 p_1 能够整除 q_1，即

$$q_1=c_1p_1.$$

因为 q_1 是质元，所以 c_1 是可逆元，因此 p_1 与 q_1 相伴，于是我们有

$$p_1p_2\cdots p_m=c_1p_1q_2\cdots q_n=p_1(c_1q_2)\cdots q_n.$$

因为 R 是主理想子环环，所以也是整环，因此把 p_1 消去就得到

$$p_2\cdots p_m=(c_1q_2)\cdots q_n.$$

这时 p_i 的个数是 $m-1$. 根据上面归纳法假设，我们有 $m-1=n-1$，所以 $m=n$，并且 p_2, …, p_m 除顺序外分别与 c_1q_2, …, q_n 相伴，已知 p_1 与 q_1 相伴，所以定理成立.

于是在主理想子环环中，元 a 如果能分解为有穷个质元的乘积，那末这有穷个质元的个数是一定的，这个数我们又叫做 a 的长.

在整数环中，可逆元只有 -1 及 1. 所以整数的质因子分解，除顺序外，相差只是一个符号. 又假如 F 是可换体，在多项式环 $F[x]$ 中，只有 F 中元是可逆元，所以这时多项式的既约分解，除顺序外，相差只是 F 中元的因子.

我们知道在整数环 Z 中，因子分解定理成立，在多项式环 $Z[x]$ 中因子分解定理也同样成立，但 $Z[x]$ 不是主理想子环环，而是关于主理想子环环 Z 的多项式环. 一般，在有单位元的整环 R 中，如果元素的因子分解定理能够成立，我们可以证明，在多项式环 $R[x]$ 中元素的因子分解定理也能够成立. 因此，在主理想子环环或关于主理想子环的多项式环中，元素的因子分解定理是成立的. 1955 年肯兹(G. Kantz)证明了它的逆定理：任一满足元素因子分解定理的环是主理想子环环或者是关于主理想子环的多项式环[21]. 这些我们在这里都不详细谈论了.

上面我们所说的环都是可换环. 关于非可换环，同样我们也

有主理想子环环及欧氏环的概念，这只要把前面定义中的交换律除去就得了．在非可换主理想子环环中，元素的因子分解定理也是成立的[22]．

在可换环中，一个理想子环除因子的顺序外能否一意地分解为质理想子环的乘积，这是所谓的理想子环分解问题，它是环论中主要问题之一．由上面的定理 7，我们容易得知，在主理想子环环中，任一异于零及自身的理想子环除因子的顺序外，能够一意分解为质理想子环的乘积，因此理想子环的分解问题，在主理想子环环中是解决了的．此外，在某些环中这问题也解决了[23]．但在一般情况下，这问题到现在还没有得到解决．

习 题 3.9

1．同余式 $6x\equiv17(19)$ 是否有解？为什么？

2．试证在所有形状象 $a+b\sqrt{-5}$，a，b 是整数，的数形成的环中，

$$9=3\cdot3=(2+\sqrt{-5})(2-\sqrt{-5})$$

是两种不可约数的分解．这就是说，在整环中，因子分解定理不一定成立．

3．在主理想子环环中，所有与 a 互质的元所在的同余类（关于模 (a)）对于乘法成群，怎样证明？

4．试证高斯数环是欧氏环．

5．假定 R 是满足因子分解定理并且有单位元 1 的整环，$f(x)=\sum_{i=0}^{n}a_ix^i$ 是 $R[x]$ 中元，d 是 a_0，a_1，$\cdots$，a_n 的最大公约元，那末我们有 $f(x)=dg(x)$，当 $d=1$ 时，$f(x)$ 叫做**本原多项式**．试证 R 中两个本原多项式的乘积仍然是本原多项式．

§ 3.10 多项式的零点

这节讨论多项式环 $R[x]$ 中多项式 $f(x)$ 零点的有关问题，它与 $R[x]$ 中元素的因子分解有关．这里 R 是有单位元的整环，所

得到的结果与普通代数中的完全一致，因此也可以说是它的推广.

我们知道 R 的扩张环中一元 α，如果满足多项式 $f(x)$，也就是说 $f(\alpha)=0$，那末 α 就叫做 $f(x)$ 的零点，或者叫做 $f(x)$ 的根. 同普通代数中一样，我们有

定理 1 α 是多项式 $f(x)$ 零点的必要充分条件是 $f(x)$ 能够用 $x-\alpha$ 整除.

证明 假如 $f(x)$ 能够用 $x-\alpha$ 整除，那末

$$f(x)=(x-\alpha)g(x),$$

因此

$$f(\alpha)=(\alpha-\alpha)g(\alpha)=0,$$

所以 α 是 $f(x)$ 的零点. 反过来，假如 α 是 $f(x)$ 的零点，因为由欧氏法式，$f(x)$ 可以写成

$$f(x)=(x-\alpha)q(x)+r,$$

于是

$$f(\alpha)=(\alpha-\alpha)q(\alpha)+r,$$

因此 $r=0$，所以 $f(x)=(x-\alpha)q(x)$，即 $f(x)$ 能够用 $x-\alpha$ 整除，于是定理得证.

一般我们有

定理 2 环 R 中互异的 m 个元 $\alpha_1, \cdots, \alpha_m$ 是多项式 $f(x)$ 零点的必要充分条件是 $f(x)$ 能够用 $(x-\alpha_1)\cdots(x-\alpha_m)$ 整除.

证明 充分性很容易证明，下面只证明它的必要性.

我们用归纳法来证明. 当 $m=1$ 时，就是上面的定理 1，因此这时定理成立. 现在假定 $m-1$ 时定理成立，即

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_{m-1})g(x),$$

于是我们有

$$(\alpha_m-\alpha_1)\cdots(\alpha_m-\alpha_{m-1})g(\alpha_m)=0,$$

但 $\alpha_m-\alpha_i\neq 0$，并且 R 是无零因子环，所以 $g(\alpha_m)=0$. 由上定理，

$$g(x)=(x-\alpha_m)q(x),$$

所以

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_{m-1})(x-\alpha_m)q(x),$$

这就是说，$f(x)$能够用$(x-\alpha_1)\cdots(x-\alpha_m)$整除，因此定理成立.

于是我们得知，假如$f(x)$是$R[x]$中n次多项式，那末它在R中互异的零点不能多于n个. 要注意的是，这里R是整环，假如R不是整环，这定理是不能成立的[24]. 譬如$Z-(6)$是有单位元的可换环，但不是无零因子环，这时多项式$f(x)=x^2-x$在其中有四个互异的零点$\bar{0}$, $\bar{1}$, $\bar{3}$, $\bar{4}$. 又如四元数体是非可换体，这时多项式$f(x)=ex^2+e$在其中有六个互异的零点$\pm i$, $\pm j$, $\pm k$.

根据上面的定理我们有

定义 假定$f(x)$能够用$(x-\alpha)^k$整除，k是大于1的整数，但不能用$(x-\alpha)^{k+1}$整除，那末α就叫做$f(x)$的k**重零点**.

在讨论重零点时，需要导函数这个概念，但极限，连续等基本概念都不能在环中引用，所以我们不能用数学分析上的定义. 我们同普通代数中一样，假如

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n,$$

那末

$$f'(x)=na_0x^{n-1}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$$

就叫做$f(x)$的**导函数**. 由定义不难证明:

$$\{f(x)+g(x)\}'=f'(x)+g'(x),$$

$$\{f(x)\cdot g(x)\}'=f'(x)g(x)+f(x)g'(x),$$

$$\{f^m(x)\}'=mf^{m-1}(x)\cdot f'(x).$$

定理 3 多项式$f(x)$有重零点α的必要充分条件是$f(x)$, $f'(x)$有公因式$x-\alpha$.

证明 假如α是$f(x)$的$k(>1)$重零点，那末

$$f(x)=(x-\alpha)^k g(x),\quad g(\alpha)\neq 0,$$

因此

$$f'(x)=(x-\alpha)^k g'(x)+k(x-\alpha)^{k-1}g(x)$$
$$=(x-\alpha)^{k-1}\{(x-\alpha)g'(x)+kg(x)\},$$

因为 $k-1>0$, 所以 $(x-\alpha)^{k-1}$ 是 $f(x)$, $f'(x)$ 的公因式. 于是条件的必要性得证.

再假如 α 是 $f(x)$ 的零点,但不是重零点,那末

$$f(x)=(x-\alpha)g(x),\quad g(\alpha)\neq 0,$$
$$f'(x)=(x-\alpha)g'(x)+g(x),$$

于是 $f'(\alpha)=g(\alpha)\neq 0$, 所以 α 不是 $f'(x)$ 的零点,也就是说 $x-\alpha$ 不是 $f'(x)$ 的因式. 因此如果 $x-\alpha$ 是 $f(x)$、$f'(x)$ 的公因式, 那末 α 是 $f(x)$ 的零点, 并且是重零点. 于是条件的充分性成立. 所以定理得证.

将来(§4.6)我们还会知道: 当 R 是整环时, $R[x]$ 中任一多项式在 R 的适当扩张体中, 至少有一零点存在, 现在我们暂时承认这性质,于是由定理 3, 即得

定理 4　多项式 $f(x)$ 有重零点的必要充分条件是 $f(x)$, $f'(x)$ 有次数大于零的公因式.

此外我们还有下面的重要定理.

定理 5　任意复系数 $n(>0)$ 次多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n,\quad a_0\neq 0,$$

至少有一个复数根.

证明　假如我们能够证明多项式的系数都是实数时定理成立,那末系数是复数时定理也成立. 这是因为,命

$$\bar{f}(x)=\bar{a}_0x^n+\bar{a}_1x^{n-1}+\cdots+\bar{a}_{n-1}x+\bar{a}_n,$$

这里 $\bar{a}_i$ 是 a_i 的共轭复数, $f(x)$ 与 $\bar{f}(x)$ 的乘积

$$F(x)=f(x)\bar{f}(x)=b_0x^{2n}+b_1x^{2n-1}+\cdots+b_{2n},$$

由实际计算,我们容易得知

$$b_k=\sum_{i+j=k} a_i\bar{a}_j,\quad k=0,\ 1,\ \cdots,\ 2n.$$

但 $\bar{b}_k=\sum_{i+j=k}\bar{a}_i a_j=b_k$, 因此 $F(x)$ 的系数都是实数，于是根据上面的假定，$F(x)$ 至少有一个复根 α, 即 $F(\alpha)=f(\alpha)\bar{f}(\alpha)=0$. 如果 $f(\alpha)\neq 0$, 那末 $\overline{\bar{f}(\alpha)}=f(\bar{\alpha})=0$, 这就是说，$\alpha$ 或者 $\bar{\alpha}$ 是 $f(x)$ 的根，因此我们只要就 $f(x)$ 的系数都是实数这种特殊情形来证明就行了.

假定 $n=2^l m$, m 是奇数，我们对于 l 用数学归纳法来证明.

当 $l=0$ 时，$f(x)$ 是奇数次多项式，这时如果 x 取适当大的正值，$f(x)$ 的符号与 a_0 的符号相同，如果 x 取绝对值适当大的负值，$f(x)$ 的符号与 a_0 的符号相反．因为 $f(x)$ 是 x 的连续函数，由数学分析我们得知，$f(x)$ 有一个实根，这就是说当 $l=0$ 时，定理成立.

现在我们假定多项式的次数能够用 2^{l-1} 整除时定理成立，我们来讨论次数 $n=2^l m$ 的情况.

根据我们暂时承认的性质，容易知道 $f(x)$ 在复数体的适当扩张体中有 n 个根，假定这 n 个根是 $\alpha_1,\ \cdots,\ \alpha_n$, 任取一实数 c, 作

$$\beta_{ij}=\alpha_i\alpha_j+c(\alpha_i+\alpha_j),\quad i<j,\quad i,\ j=1,\ 2,\ \cdots,\ n.$$

这时 β_{ij} 的个数是

$$\frac{n(n-1)}{2}=\frac{1}{2}\,2^l m(2^l m-1)=2^{l-1}m',\quad m' \text{ 是奇数},$$

于是多项式

$$g(x)=\prod_{i<j}(x-\beta_{ij}),\quad i,\ j=1,\ 2,\ \cdots,\ n$$

的次数是 $2^{l-1}m'$, 由中学代数我们容易得知，它的系数是 β_{ij} 的初等对称多项式，当然也是 α_i 的对称多项式．但 α_i 的初等对称多项式是 $f(x)$ 的系数，因此它们都是实数，所以 $g(x)$ 的系数也都是实数．根据归纳法的假设，$g(x)$ 至少有一个复数根，即 β_{ij} 中至少有一个是复数，也就是说，对于任一实数 c, 我们至少有一个复数 β_{ij}, 但实数的个数是无穷，而 $i,\ j$ 只有 $\dfrac{n(n-1)}{2}$ 对，因此在上面这些

复数中,有 i, j 相同,而实数 c 不相同的复数

$$\alpha=\alpha_i\alpha_j+c_1(\alpha_i+\alpha_j),\quad \beta=\alpha_i\alpha_j+c_2(\alpha_i+\alpha_j),$$

由于

$$\alpha_i+\alpha_j=\frac{\alpha-\beta}{c_1-c_2},\quad \alpha_i\alpha_j=\frac{c_1\beta-c_2\alpha}{c_1-c_2}$$

都是复数,所以 α_i, α_j 是复系数多项式

$$x^2-(\alpha_i+\alpha_j)x+\alpha_i\alpha_j=0$$

的根. 显然 α_i, α_j 也都是复数,这就是说 $f(x)$ 至少有一个复数根,因此定理得证.

上定理就是我们普通所谓的**代数基本定理**. 远在 1629 年,吉拉尔 (A. Girard, 1595～1632) 就有此预想, 1746 年达朗贝尔 (J. E. R. D'Alembert, 1717～1783) 首先给了一个证明,但是不够严格,直到 1799 年高斯才圆满的解决了这问题. 此后高斯又给出了另外三个证明,上面的证明基本上就是他的第二个证明[35].

习 题 3.10

1. 假如 $R=Z-(5)$, 试求 $R[x]$ 中多项式 x^5-1 在 R 中的零点.
2. 假如 a 是 $f(x)$ 的 k 重零点,试证 a 是 $f'(x)$ 的 $k-1$ 重零点.
3. 假定 m 是 n 的约数,试证 x^m-1 是 x^n-1 的因式.
4. 假定 R, R' 是有单位元并且元数是无穷的整环, R' 是 R 的扩张环, $f(x_1, \cdots, x_n)$ 是多项式环 $R'[x_1, \cdots, x_n]$ 中多项式,如果 $f(x_1, \cdots, x_n)\neq 0$,试证 R 中有元 $a_1, \cdots, a_n$ 使 $f(a_1, \cdots, a_n)\neq 0$.

参 考 文 献

[1] Passman, D. S. What is a group ring? Amer. Math. Monthly, 83 (1976), no. 3, 173～185.

[2] Gilmer, Robert, A note on rings with only finitely many subrings, Scripta Math., 29 (1973), 37～38.

[3] (1) R. Bear, Inverses and zero divisors, Bull. Amer. Math. Soc., 48(1942),

630～638.

(2) N. Jacobson, Some remarks on one-side inverses, Proc. Amer. Math. Soc., 1 (1950), 352～355.

(3) M. Osima (大岛), Note on inverse in Rings, J. Gakugei Tokushima Univer., 3 (1953), 21～23.

(4) C. W. Bitzer, Inverses in rings with unity, Amer. Math. Monthly, 70 (1963), 315.

[4] (1) N. Ganesan, Properties of rings with a finite number of zero divisors I, Math. Ann., 157 (1964), 215～218; II, Math. Ann., 161 (1965), 241～246.

(2) Mcdonald, Bernard R, Finite rings with unity.

[5] N. Jacobson, Structure of rings (1956), 186.

[6] Hua Loo-kang(华罗庚), On the Automorphisms of a sfield, Proc. Nat. Acad. Sci. U. S. A., 35 (1949), 386～389.

[7] A. Malcev, On the immersion of an algebraic ring into a field, Math. Ann., 113 (1936), 686～691.

[8] N. Jacobson, The theory of rings (1943), 31.

[9] O. Ore, Linear equations in non-commutative fields, Ann. of Math., 32 (1931), 463～477.

[10] N. H. McCoy, Remarks on divisors of zero, Amer. Math. Monthly, 49 (1942), 286～295.

[11] W. R. Scott, Divisors of zero in polynomial rings, Amer. Math. Monthly, 61 (1954), 336.

[12] N. H. McCoy, Annihilators in polynomial rings, Amer. Math. Monthly, 64 (1957), 28～29.

[13] N. H. McCoy, The theory of rings (1967), 37～38.

[14] Kruse, Robert L., Rings in which all subrings are ideals I, Canad J. Math., 20 (1968), 862～871.

[15] O. Steinfeld, On Ideal-quotients and prime ideals, Acta Math. Acad. Sci. Hung., 6 (1953), 289～298.

[16] N. H. McCoy, Prime ideals in general rings, Amer. Jour. of Math., 71 (1949), 823～833.

[17] N. H. McCoy, The Theory of rings (1967), 72～73.

[18] Sands, Arthur D., Prime ideals in Matrix rings, Proc. Glasgow Math. Assoc., 2 (1956), 193～195.

[19] (1) N. J. Divinsky, Rings and radicals (1965), §3.4.

(2) R. E. Johnson, Prime rings, Duke Math. J., 18 (1951), 799～809.

[20] (1) T. S. Matzkin, The Euclidean algorithm, Bull. Amer. Math. Soc., 55

(1949), 1142～1146.

(2) H. H. Brungs, Left Euclidean rings, Pacific J. Math., 45 (1973), 29～37.

[21] (1) G. Kantz, Über den Typus eines Zerlegungs Rings, Monatsh Math., 59 (1955), 104～110.

(2) ——, Über Integrilats bereich mit eindeutiger Primelementzarlegung, Arch. Math., 6 (1955), 397～402.

[22] N. Jacobson, The theory of rings (1943), 34.

[23] B. L. Von der Waerden, Zur Produktzerlegung der Ideal in ganz-abgeschlessenen Ringen, Math. Ann., 101 (1929), 293～308.

[24] R. A. Beaumont, Equivalent properties of a ring, Amer. Math. Monthly, 57 (1950), 183.

[25] H. Zassenhaus, On the fundamental theorem of algebra, Amer. Math. Monthly, 74 (1967), 485～496.

第四章

可换体论

体的基本概念在上章已作了简单介绍，这章将详细讨论可换体的构造．因为任一体可以看成为它的子体的扩张体，它可以由子体添加若干元而成，所以我们讨论体的构造从扩张入手，先讨论代数扩张体，再讨论超越扩张体，我们的重点在代数扩张体而且以有穷的为主．

关于可换体的构造，斯太尼兹 (E. Steinitz, 1871～1928) 于 1910 年在 Crelle 杂志上发表长达 142 页的论文，详加论述．1930 年这长篇大论另发行单行本，是可换体论的经典著作[1]．1952 年斯那泼尔 (E. Snapper, 1913～) 曾把斯太尼兹这套理论应用到完全准质环*)上，建立了完全准质环的构造，读者如有余力，可参考文献[2]．

要注意的是，这里只是可换体的构造．关于一般体的构造虽然也有大量的结果[3]，但大部分都是特殊情况，一般结论，至今尚未能求得．

§4.1 添　　加

我们知道，假如体 K 的子集 F 对于 K 的两种结合法又形成

*) 一个可换环如果有单位元，并且它的根基是极大理想子环，它就叫做完全准质环．也就是说，假如可换环 R 有单位元，D 是它的根基，如果 $R-D$ 成体，那末 R 就是完全准质环．显然，体是完全准质环．

为体，就叫做 K 的**子体**．这时 K 又叫 F 的**扩张体**．K 自身可以看成为自己的子体．由 §2.2 我们又知道，体 K 的子集 F 形成为子体的必要充分条件是

1° F 含有非零的元；

2° 假如 $a, b\in F$，那末 $a-b\in F$，并且当 $b\neq 0$ 时，$ab^{-1}\in F$.

假如 K 是体 F 的扩张体，L 是 K 的子体，并且又是 F 的扩张体，即 $K\supseteq L\supseteq F$，那末 L 叫做 K，F 的**中间体**．假如 M 是 K 的子集，显然在 K，F 的中间体中有包含 M 的中间体存在，因为 K 自身就是这样的一个中间体．在 K，F 的中间体中，所有包含 M 的交集又是包含 M 的中间体，因此它就是 K 中包含 F 及 M 的最小子体．这体我们用 $F(M)$ 来表示，叫做 **F 添加 M 扩张的体**．当 $M=\{u_1, \cdots, u_n\}$ 时，我们又用记号 $F(u_1, \cdots, u_n)$ 表示．在 §3.5 中，环的添加是用方括弧表示，这里体的添加我们用圆括弧．显然，

$$F\subseteq F(M)\subseteq K,\ F(K)=K,$$

当 $M\subseteq F$ 时，

$$F(M)=F.$$

我们知道 $F(M)$ 包含 F 及 M 的元，因此包含 F 中元与 M 中元的一切有理结合(加，减，乘，除)．但所有这些有理结合的元自身显然形成为一个体，因为它包含 F 及 M，所以它就是 $F(M)$．这就是说，$F(M)$ 是由 F 中元与 M 中元的一切有理结合的元形成的体．当 K 可换时，$F(M)$ 中元就是 M 中元的有理函数，它的系数是 F 中元．

因为在 F 中元及 M 中元的任一有理结合中，M 中元只出现有穷个，所以 $F(M)$ 中任意元包含在 M 的某有穷子集 N 的添加 $F(N)$ 中，因此 $F(M)$ 是若干个有穷集添加的并集．这也就是说，任意集的添加可以由有穷集添加的并集形成．

再假如 M_1, M_2 是 K 的子集，显然

$$F(M_1)(M_2)=F(M_2)(M_1),$$

又

$$F(M_1\cup M_2)=F(M_1)(M_2),$$

这是因为，$F(M_1\cup M_2)$包含 F 及 M_1, M_2，于是也包含 $F(M_1)$及 M_2，因此包含 $F(M_1)(M_2)$，所以 $F(M_1\cup M_2)\supseteq F(M_1)(M_2)$. 反过来，$F(M_1)(M_2)$包含 $F(M_1)$及 M_2，于是也含 F 及 $M_1\cup M_2$，因此 $F(M_1)(M_2)\supseteq F(M_1\cup M_2)$. 所以 $F(M_1\cup M_2)=F(M_1)(M_2)$. 于是我们得知，$F(u_1, \cdots, u_n)=F(u_1)\cdots(u_n)$. 即有穷集的添加可以由有穷多回陆续添加一个元而得，因此一个元的添加如果研究清楚了，那末任意集的添加也可以说基本上清楚了. 所以一个元的添加是最基本的，我们叫它做**单扩张**. 假如 K 是 F 的单扩张体 $K=F(\alpha)$，这 α 我们又叫做 K 关于 F 的**本原元**.

§4.2 质体，特征数

因为我们讨论体的构造是由子体的添加入手，所以我们首先来讨论体的最小子体，即所谓质体的构造.

同讨论群、环时一样，体 K 的所有子体(包含自身)的交集仍然是子体，这子体显然除自身外不再包含其他子体. 象这样只有自身做子体的体，叫做**质体**. 因此，任意体都含有质体做它的子体.

再假如 K 有两个互异的质体 F_1, F_2, 因为 $F_1\cap F_2$ 也成为体，所以 F_1, F_2 就有异于自身的子体，这与 F_1, F_2 是质体的假设不合，因此在 K 的子体中是质体的只有唯一个，于是我们得到

定理 1 任意体包含一个而且只一个质体.

单位元群是只有自身做子群的群，零环是只有自身做子环的环，任意群包含单位元群，任意环也包含零环. 在这点上，质体与

单位元群、零环类似.

我们容易得知有理数体 Q 是质体,整数环 Z 关于质数 p 的同余环 $Z-(p)$ 也是质体. 下面我们来证明一般的质体只有这两种类型.

假如 F 是质体,e 是它的单位元,那末

$$(1)\qquad \cdots,\ -2e,\ -e,\ 0,\ e,\ 2e,\ \cdots$$

都是 F 中元,它们形成整环 R,结合法是:

$$me+ne=(m+n)e,\quad me\cdot ne=mne.$$

同 §2.2 中讨论循环群的构造一样,下面分两种情形来讨论.

1. 假如(1)中元都互不相等,也就是说当 $ne=0$ 时,$n=0$. 那末 R 与整数环 Z 同构,但 Z 的商体是有理数体 Q,因此 R 的商体也就与有理数体 Q 同构,这就是说,F 含有与 Q 同构的子体,所以这时 $F\cong Q$.

2. 假如(1)中元有相等的,也就是说,有非零的整数 n 适合 $ne=0$. 假如 p 是适合 $pe=0$ 的最小正整数,那末 p 是质数,这是因为,如果 $p=mn$,那末

$$pe=mne=me\cdot ne=0,$$

因此 $me=0$ 或 $ne=0$,这与 p 是最小的性质不合. 同 §2.2 中一样,(1)中任意元与

$$0,\ e,\ \cdots,\ (p-1)e$$

中某一元相等,由 §3.2,我们得知这 p 个元形成一个可换体,它与 $Z-(p)$ 同构. 这就是说 F 有与 $Z-(p)$ 同构的子体,所以这时 $F\cong Z-(p)$.

一个体,它的单位元 e 的任意倍如果都异于零,象第 1 种情形那样,我们叫这体的**特征数是零**. 如果 e 的某质数 p 倍是零,象第 2 种情形那样,我们就叫这体的**特征数是** p. 也就是说,假如我们把体看成加群,如果它的单位元 e 的阶是无穷,那末它的特征数就

是零；如果 e 的阶是有穷，并且是某质数 p，那末它的特征数就是 p.

譬如有理数体、实数体、复数体及四元数体的特征数都是零，而 $Z-(p)$ 的特征数是 p.

引用特征数这个概念，由上面的讨论，我们得到

定理 2 质体的特征数如果是零，它与有理数体 Q 同构，如果是 p，它与整数环 Z 关于 (p) 的同余环 $Z-(p)$ 同构.

假定 F 是体 K 的子体，因为 F 的单位元就是 K 的单位元，所以 F 的特征数与 K 的特征数一致. 这就是说，体与它的子体的特征数是相等的. 因此体 K 的特征数如果是零，它包含的质体与 Q 同构，如果是 p，它包含的质体与 $Z-(p)$ 同构.

由定理 2 显然质体是可换体.

特征数这概念是体的一个重要概念，它对于体的构造有决定性的作用. 下面我们再来讨论它的基本性质.

假定 a 是体 K 中任意非零的元，n 是整数，K 的特征数如果是零，那末由 $na=0$，我们就有 $na\cdot a^{-1}=ne=0$. 所以 $n=0$. 因此这时 $na=0$ 的必要充分条件是 $n=0$. K 的特征数如果是 p，那末 $pa=pe\cdot a=0$. 假如 $na=0$，同 §2.2 中一样，由 $n=qp+r$，$na=qpa+ra=0$，我们就有 $r=0$，所以 $n\equiv 0(p)$. 因此这时 $na=0$ 的必要充分条件是 $n\equiv 0(p)$. 一般，当 K 的特征数是零时，$ma=na$ 的必要充分条件是 $m=n$. 当 K 的特征数是 p 时，$ma=na$ 的必要充分条件是 $m\equiv n(p)$.

于是体 K 的特征数如果是零，那末 K 中任意非零元的任意倍都异于零，如果是 p，那末 K 中任意元的 p 倍都是零. 因此特征数根据定义虽然是单位元的性质，但它也是体中任意元的公共性质.

普通代数中讨论的数是实数或复数，它们都是特征数为零的

体中元. 在特征数是 p 的体中,有些运算方法就与普通不同,下面的公式就是普通代数中所不允许的.

定理 3 假设可换体 K 的特征数是 p, 而 a, b 是其中任意两元,那末

$$(a+b)^p=a^p+b^p,\quad (a-b)^p=a^p-b^p.$$

证明 因为 K 是可换体,我们有

$$(a+b)^p=a^p+C_1^pa^{p-1}b+\cdots+C_{p-1}^pab^{p-1}+b^p,$$

式中 $C_i^p=\dfrac{p(p-1)\cdots(p-i+1)}{i!}$, $1\leqslant i\leqslant p-1$. 但 C_i^p 是整数, 其中 p 又不能消去, 所以 C_i^p 能够用 p 整除, 即 $C_i^p\equiv 0(p)$, 于是 $C_i^pa^{p-i}b^i=0$,因此

$$(a+b)^p=a^p+b^p.$$

假如命 $a-b=a'$, 即 $a=a'+b$, 那末 $a^p=a'^p+b^p$, 因此

$$(a-b)^p=a^p-b^p,$$

所以定理得证.

1963 年卡斯拉(S. Caslar)证明了上定理的逆,即假如体 K 的特征数是 p, 如果对于 K 中任意元 a, b, 我们有 $(a+b)^p=a^p+b^p$, 那末 K 是可换体[4]. 因此特征数是 p 的体是可换体的必要充分条件是: 对于其中任意元 a, b, 有 $(a+b)^p=a^p+b^p$.

显然, 体的特征数又是把体看成加群时其中任意非零元的阶数. 环也可看作为加群,因此我们可以把特征数这个概念推广到环上面来.

环 R 看成加群时, 元素的阶数如果没有最大数, 我们就说 R 的特征数是零; 如果最大数是正数 m, 我们就说 R 的特征数是 m. 因此,假如 R 有单位元 e, 当 e 的阶是无穷时, 显然这时 R 的特征数是 0; 当 e 的阶数是 m 时,因为对于 R 中任意元 a,

$$ma=m(ea)=(m\cdot e)a=0\cdot a=0,$$

也就是说，任意元的阶数不大于 m，所以这时 R 的特征数是 m. 于是，有单位元环的特征数概念也可以与体一样来定义.

假如 R 是无零因子环，a, b 是其中非零的两元，那末由 $ma=0$，我们就有 $mb=0$，这是因为

$$(mb)a=b(ma)=0,$$

而 $a\neq 0$，所以 $mb=0$. 这就是说，在无零因子环中，所有非零元的阶数是一致的. 因此无零因子环的特征数就是其中所有非零元的公共阶数. 再我们又容易得知，无零因子环的特征数与体的特征数一样，或是零，或者是质数.

要注意的是，虽然体的特征数与它的子体的特征数相同，但环与它的子环不一定有相同的特征数. 譬如在 §3.4 习题 3 中，$R+Z$ 的特征数是 0，假如 R 的特征数是 p，那末 $R+Z$ 的特征数与它的子环 R 的就不同.

习　题　4.2

1. 假如 F 是体 K 的质体，试证 F 是 K 的中心的子体.
2. 试求 $Z[i]-(1+i)$ 的特征数，这里 $Z[i]$ 是高斯数环.
3. 假设体 K 的特征数是 p，试证

$$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n},\quad a,\ b\in K,$$

$$(a_1+a_2+\cdots+a_n)^p=a_1^p+a_2^p+\cdots+a_n^p,\quad a_i\in K.$$

4. 假定在特征数是 p 的体 K 中，任意元满足多项式 $x^p-x=0$，试证

$$K\cong Z/(p).$$

5. 试证布尔环是可换环，并证明它的特征数是 2.

§4.3　单扩张体

因为任意体可以从质体的添加而成，而质体的构造已经清楚，因此现在就需要讨论单扩张体了.

前面两节的讨论是对一般体而言，这节所说的体都是可换体．下面我们来讨论可换体 F 的单扩张体 $F(\alpha)$ 的构造．

假设 K 是 F 的可换扩张体*)，α 是 K 中元，因为 $F(\alpha)$ 是 K 中包含 F 及 α 的最小子体，并且 $F(\alpha)$ 包含由所有 α 的多项式 $\sum a_i\alpha^i$，$a_i\in F$，形成的环 R，这环因为在体中，所以是整环．因此，如果 R 成体，那末 R 就是 $F(\alpha)$；如果 R 不成体，那末 R 的商体就是 $F(\alpha)$．

我们把 R 与多项式环 $F[x]$ 来比较．显然对应

$$\sum a_ix^i\to\sum a_i\alpha^i$$

是 $F[x]$ 射到 R 上的同态．由 §3.6 定理 6，我们有

$$R\cong F[x]-N,$$

这里 N 是同态核，它是由 $F[x]$ 中所有以 α 为零点的多项式形成的理想子环．因为 R 是整环，所以 $F[x]-N$ 也是整环，因此 N 是 $F[x]$ 的质理想子环．再因为 N 是 R 中零元在 $F[x]$ 的完全象源，而上面的对应关系不使 F 中任意元变动，所以 N 不能是单位理想子环．但 $F[x]$ 是主理想子环环，因此由 §3.9，N 是零理想子环或者是次数大于零的既约多项式生成的质理想子环．假如 $F[x]$ 中除零元外，没有以 α 为零点的多项式，那末 $N=0$；假如 $g(x)$ 是 $F[x]$ 中以 α 为零点的既约多项式，那末 $N=(g(x))$．

1．当 $N=0$ 时，

$$R\cong F[x],$$

因此 R 的商体就是 $F(\alpha)$．但 R 的商体与 $F[x]$ 的商体同构，而 $F[x]$ 的商体是由未定元 x，系数是 F 中元的所有有理函数形成的有理函数体 $F(x)$，所以这时单扩张体 $F(\alpha)$ 与有理函数体 $F(x)$ 同构．

2．当 $N=(g(x))$ 时，因为 $g(x)$ 是既约多项式，由 §3.9 定理

*) 如果 K 不是可换体，只要 α 与 F 中任意元能够交换，下面的讨论同样成立．

6，$(g(x))$是极大理想子环，再由§3.8定理1，$F[x]-(g(x))$是体，因此R也是体，所以这时单扩张体$F(\alpha)$就是R.

当$N=0$时，α是F的超越元，因此$F(\alpha)$叫做F的**超越单扩张体**. §3.5中多项式环$R[x]$可说是环R的超越单扩张环. 当$N=(g(x))$时，α是F的代数元，因此$F(\alpha)$叫做F的**代数单扩张体**，这时$F[x]$中α所适合的既约多项式$g(x)$的次数又叫做α关于F的**次数**. 根据欧氏法式，我们不难得知，$F[x]$中α所适合的既约多项式也是$F[x]$中α所适合的次数最低的多项式. 因此$F[x]$中α所适合的既约多项式除相伴外是唯一的. 引用这定义，由上面的讨论，我们有

定理1 假定可换体K是F的扩张体，α是K中元，如果α是F的超越元，那末F的超越单扩张体$F(\alpha)$与未定元x的有理函数体$F(x)$同构. 如果α是F的代数元，那末F的代数单扩张体$F(\alpha)$与$F[x]-(g(x))$同构，这里$g(x)$是$F[x]$中α所适合的既约多项式.

在超越单扩张体$F(\alpha)$中，任意元是α的有理函数，由前面的对应关系，我们知道它的运算法则与把α看成未定元x时一样. 在代数单扩张体$F(\alpha)$中，任意元是α的多项式，假如α关于F是n次，也就是说，多项式$g(x)$是n次时，因为任意多项式$f(x)$用$g(x)$来除，得到的余式或是零，或是次数小于n的多项式，因为$g(\alpha)=0$，所以α的任意多项式$f(\alpha)$可以表为$\sum_{i=0}^{n-1} a_i\alpha^i$，$a_i\in F$形状. 再我们知道，这种表示又是一意的，这是因为，如果

$$\sum_{i=0}^{n-1} a_i\alpha^i=\sum_{i=0}^{n-1} b_i\alpha^i,$$

那末

$$\sum_{i=0}^{n-1}(a_i-b_i)\alpha^i=0,$$

但α的次数是n，所以α不能适合$F[x]$中次数小于n的多项式，

因此 $a_i=b_i$, $i=0, \cdots, n-1$. 于是 $F(\alpha)$中任意元可以一意地表为次数小于 n 的 α 的多项式. 由前面的对应关系, 我们得知这时 $F(\alpha)$ 中元的运算法则与把 α 看成为未定元 x 时的多项式的运算法则一样, 只是当运算的结果是次数不小于 n 的 α 的多项式时, 我们要引用 $g(\alpha)=0$ 把它化为 $\sum_{i=0}^{n-1} a_i\alpha^i$ 的形式, 也就是说, 把 α 看成为 x 时, $F(\alpha)$ 中元的运算法则与 $F[x]$ 中多项式的一样, 只是我们要对 $g(x)$ 取同余式就是了.

譬如 Q 是有理数体, $\alpha=\sqrt{2}$, 那末 $Q(\sqrt{2})$ 中任意元可以一意地表为 $a+b\sqrt{2}$, 这里 a, b 是有理数. 例如,

$$\frac{3+5\sqrt{2}}{4+\sqrt{2}}=\frac{(3+5\sqrt{2})(4-\sqrt{2})}{4^2-2}=\frac{1}{7}+\frac{17}{14}\sqrt{2}.$$

上面的讨论是假定 α 在 F 的扩张体 K 中, 因此 α 与 F 的结合法是已知的. 假如这包含 α 及 F 的扩张体 K 不是已知, 我们也可以仿照上面的方法来做单扩张 $F(\alpha)$, 这时 α 是 F 的超越元或者是代数元, 也就是说, α 不适合 $F[x]$ 中任意多项式或者是适合 $F[x]$ 中某既约多项式.

假如 α 是 F 的超越元, 如果超越单扩张体 $F(\alpha)$ 已做成, 由定理 1, 它与未定元 x 的有理函数体 $F(x)$ 同构, 因此我们可以根据前面的对应关系, 从 $F(x)$ 来做出所求的 $F(\alpha)$. 这只要用 α 代替 $F(x)$ 中的 x 就得到包含 α 及 F, 并且与 $F(x)$ 同构的体. 因此它就是 $F(\alpha)$, 也就是说, $F(\alpha)$ 是由系数是 F 中元的 α 的有理函数形成的体, 它的结合法与有理函数体 $F(x)$ 的完全一样, 所以 α 的有理函数体就是所求的超越单扩张体 $F(\alpha)$.

假如 α 是 F 的代数元, $g(x)$ 是 $F[x]$ 中它所适合的既约多项式, $g(x)$ 的次数我们可以假定大于 1, 因为如果是 1, 那末 $F(\alpha)=F$, 也就是说 $F(\alpha)$ 就是 F 了. 同上面一样, 如果代数单扩张体 $F(\alpha)$ 已做成, 由定理 1, 它与 $F[x]-(g(x))$ 同构, 因此我们可以根

据前面的对应关系，从 $F[x]-(g(x))$ 来做出所求的 $F(\alpha)$. 我们知道，$F[x]$ 中多项式 $f(x)$ 与 $F[x]-(g(x))$ 中的同余类 $\overline{f(x)}$ 对应是 $F[x]$ 射到 $F[x]-(g(x))$ 上的同态，但不是同构. 假如在 $F[x]$ 中我们只考虑 F 中元，那末上面的同态 $a\rightarrow\bar{a}$ 就是同构. 这是因为，当 $a\neq b$ 时，$a\not\equiv b\,(g(x))$，因此 $F[x]-(g(x))$ 中包含与 F 同构的子体. 引用 §3.3 的挖补定理，我们就得到包含 F 并且与 $F[x]-(g(x))$ 同构的体 K. 再因为 $g(x)$ 的次数大于 1，所以在体 K 中，x 所在的陪集 $\bar{x}$ 不是 F 中元，我们用 α 来代替陪集 $\bar{x}$. 于是 K 就是由系数是 F 中元的 α 的多项式形成的体，它包含 α 及 F 并且与 $F[x]-(g(x))$ 同构. 我们假定 $g(x)=\sum a_i x^i$，那末在 $F[x]-(g(x))$ 中，

$$\overline{g(x)}=\sum\overline{a_i x^i}=\sum\bar{a}_i\bar{x}^i=\bar{0},$$

当 a_i 代替 $\bar{a}_i$，α 代替 $\bar{x}$ 时，我们就有 $\sum a_i\alpha^i=0$，因此在 K 中，$g(\alpha)=0$. 这就是说，α 与 F 中元的结合法象上面那样来规定时，α 就是 $g(x)$ 的零点，所以 K 就是代数单扩张体 $F(\alpha)$.

于是我们有

定理 2 假定 F 是可换体，α 是元素，我们有 α 是 F 的超越元的超越单扩张体 $F(\alpha)$，它与 $F(x)$ 同构，也有 α 是 $F[x]$ 中既约多项式 $g(x)$ 的零点的代数单扩张体 $F(\alpha)$，它与 $F[x]-(g(x))$ 同构.

这定理的结论与定理 1 的完全一致，唯一的差别是在包括体 K 是否已知. 要注意的是代数单扩张体 $F(\alpha)$ 的构造是由 α 适合的既约多项式 $g(x)$ 一意确定的.

一般添加 $\alpha_1, \cdots, \alpha_n$ 于可换体 F 扩张的体 $F(\alpha_1, \cdots, \alpha_n)$ 也可以同样求得. 因为添加 $\alpha_1, \cdots, \alpha_n$ 于 F 扩张的体就是每回添加一元陆续添加 $\alpha_1, \cdots, \alpha_n$ 于 F 扩张的体. 当 $\alpha_1, \cdots, \alpha_n$ 中有 F 的超越元时，$F(\alpha_1, \cdots, \alpha_n)$ 中任意元是系数是 F 中元的 $\alpha_1, \cdots, \alpha_n$ 的有理函数；当 $\alpha_1, \cdots, \alpha_n$ 都是 F 的代数元时，$F(\alpha_1, \cdots, \alpha_n)$ 中任意

元是系数是 F 中元的 $\alpha_1, \cdots, \alpha_n$ 的多项式。

现在我们来讨论两个单扩张之间的关系，为了更好地说明，我们引进一个新概念.

定义 假如 K, K' 都是体 F 的扩张体，σ 是 K 射到 K' 上的同构，如果

$$\sigma(a)=a, \quad a\in F,$$

也就是说，σ 不使 F 中任意元变动，那末 σ 叫做 K, K' 关于 F 的同值，这时 K, K' 又叫做关于 F 同值.

譬如 $a+bi\to a-bi$, a, b 是实数，就是复数体关于实数体的自同值.

假如 $F(\alpha)$, $F(\beta)$ 是 F 的超越单扩张体，因为 $F(\alpha)$, $F(\beta)$ 与 $F(x)$ 不只都是同构，而且关于 F 又都是同值，因此 $F(\alpha)$, $F(\beta)$ 关于 F 同值，它们的同值映射是不使 F 中任意元变动而把 α 变为 β.

假如 $F(\alpha)$、$F(\beta)$ 是 F 的代数单扩张体，并且 α, β 是 $F[x]$ 中同一个 n 次既约多项式 $g(x)$ 的零点. 因为这时 $F(\alpha)$ 与 $F(\beta)$ 都与 $F[x]-(g(x))$ 同构，所以 $F(\alpha)$ 与 $F(\beta)$ 同构，由前面的对应关系我们容易知道

$$\sum_{i=0}^{n-1} a_i\alpha^i\to\sum_{i=0}^{n-1} a_i\beta^i$$

就是它们的同构映射，这映射不使 F 中任意元变动，并且把 α 变为 β, 因此 $F(\alpha)$ 与 $F(\beta)$ 关于 F 同值.

由上面的讨论，我们得

定理 3 假设 $F(\alpha)$, $F(\beta)$ 是可换体 F 的单扩张体，如果 α, β 都是 F 的超越元，那末 $F(\alpha)$、$F(\beta)$ 关于 F 同值；如果它们都是 F 的代数元，并且又都是 $F[x]$ 中同一既约多项式的零点，那末 $F(\alpha)$, $F(\beta)$ 关于 F 同值. 上面这两种同值都有不使 F 中任意元

变动而把 α 变为 β 的同值映射.

我们知道,代数单扩张体的本原元不是唯一的,所以代数单扩张 $F(\alpha)$, $F(\beta)$ 关于 F 同值时,α, β 不一定就是 $F[x]$ 中同一既约多项式的零点. 因此它们的同值映射不一定就把 α 变为 β. 譬如 Q 是有理数体,因 $Q(\sqrt{2})=Q(2\sqrt{2})$, 当然 $Q(\sqrt{2})$, $Q(2\sqrt{2})$ 关于 Q 同值, 但 $\sqrt{2}$, $2\sqrt{2}$ 不是 $Q[x]$ 中同一既约多项式的零点,因此它们没有把 $\sqrt{2}$ 变为 $2\sqrt{2}$ 的自同值映射.

在 §2.4 中, 我们介绍了群的共轭元及共轭子群的概念,在体中我们也有与这类似的概念.

假定 K 是 F 的扩张体, L_1, L_2 是 K, F 的中间体,如果它们关于 F 同值,那末 L_1, L_2 就叫做关于 F **共轭**. 这时 L_1 中元 α_1 在 L_2 中的象 α_2, 叫做 α_1 关于 F 的**共轭元**,而 α_1, α_2 又叫做关于 F **共轭**. 因此 F 中元与自身共轭. 再从定理 3, 我们容易得知 F 的任意两个超越元是 F 的共轭元; F 的代数元成为共轭的必要充分条件是它们为 $F[x]$ 中同一既约多项式的零点.

下面是关于多项式零点的**克罗纳克尔**(L. Kronecker, 1823~1891) **定理**.

定理 4 假如 $f(x)$ 是多项式环 $F[x]$ 中多项式, 那末在体 F 的扩张体中,有包含 $f(x)$ 的零点的体存在.

证明 假设 $g(x)$ 是 $f(x)$ 在 $F[x]$ 中的既约因式, 那末把 $g(x)$ 的零点 α 添加于 F 得到的单扩张体 $F(\alpha)$, 也就是说, 与 $F[x]-(g(x))$ 同构的体就是所求的体,因此定理成立.

假如 $F[x]$ 中任意多项式的零点都在 F 中, 那末 F 叫做**代数闭体**. 因此, 如果 F 是代数闭体, 那末 $F[x]$ 中任意既约多项式的次数都是 1, 于是添加 F 的任意代数元于 F 得到的扩张体仍然是 F 自身, 也就是说, 这时 F 不能够再用代数扩张来扩大. 譬如复数体就是代数闭体,这是因为根据代数基本定理(§3.10), 任意系

数是复数的多项式的零点仍然是复数，因此复数体不能再用代数扩张来扩大.

引用冲恩(M. Zorn)引理*)，我们不难证明任意体可以代数扩张成为代数闭体，并且假如体 F 的扩张体 K, K' 都是代数闭体，那末 K, K' 关于 F 同值[6].

习 题 4.3

1. 假如 α 是 $Q[x]$ 中既约多项式 $g(x)=x^2-5x+7$ 的零点，试把

$$\frac{1-7\alpha+2\alpha^2}{1+\alpha-\alpha^2}$$

写成 α 的多项式，这里 Q 是有理数体.

2. 试求 $Q(\sqrt[3]{2})$ 中元 $1+\sqrt[3]{2}+\sqrt[3]{4}$ 的逆元.

3. 假定 Q 是有理数体，试证 $Q(i)\simeq Q[x]-(x^2+1)$.

4. 假如 F 是实数体，α 是既约多项式 $g(x)=x^2+x+1$ 的零点，求作代数单扩张体 $F(\alpha)$，并且在 $F(\alpha)$ 中分解 $g(x)$ 为既约因式的乘积.

5. 假如 F 是特征数为 p 的质体，x 是未定元，$K=F(x)$，试求将既约多项式 y^p-x 的一零点 $\alpha=x^{\frac{1}{p}}$ 添加于 K 所得的扩张体 $K(\alpha)$，并且在 $K(\alpha)$ 中分解 y^p-x.

6. 假如 $f(x)$, $p(x)$ 是 $F[x]$ 中多项式，并且 $p(x)$ 是既约的，如果在 F 的扩张体 K 中，$f(x)$, $p(x)$ 有公共零点，试证 $f(x)$ 能够用 $p(x)$ 整除.

7. 假如多项式环 $F[\alpha]$ 是体，那末 $F[\alpha]$ 是 F 的代数体.

§4.4 向量空间，代数

在讨论添加代数元扩张的体时，需要向量空间的一些概念和性质，这节我们先从广泛的向量空间开始. 因为"代数"是环、体中重要的一类，而且又是特殊的向量空间，所以最后我们对代数也作

*) 假定 M 是由某集合的若干子集形成的系，L 是 M 的子集，如果 L 中任意两元 L_1, L_2 不是 $L_1\subseteq L_2$ 便是 $L_2\subseteq L_1$，那末 L 叫做 M 的链，冲恩引理：假定 M 的每个链中元的并集仍是 M 中元，那末 M 中有不包含于其他元的元，即极大元.

简单介绍.

在线代数中，我们已经知道向量空间的基本概念和性质，现在我们把这些概念来推广.

定义 1 假定 V 是加群，它的元用 $u, v, \cdots$ 表示，F 是体，它的元用 $a, b, \cdots$ 表示，如果 a, u 的乘积 au 具备下列各性质，那末 V 叫做 F 的(左)向量空间，有时又简单地叫做 F 空间：

1° $au \in V$, $\quad$ 2° $a(u+v) = au + av$,

3° $(a+b)u = au + bu$, $\quad$ 4° $(ab)u = a(bu)$,

5°*) $1 \cdot u = u$.

譬如复数体、四元数体都是实数体的向量空间. 假如 K 是体 F 的扩张体，那末 K 是 F 的向量空间. 又多项式环 $F[x]$ 也是 F 的向量空间.

由定义，我们有 $(-a)u = a(-u) = -(au)$；此外，$0u = a0 = 0$. 再假如 $au = 0$，那末 $a = 0$ 或 $u = 0$，因此当 $u \neq 0$ 时，如果 $au = bu$，那末 $a = b$.

假如 V 是 F 的向量空间，如果 U 是 V 的子群，又是 F 的向量空间，那末 U 叫做 V 的子空间. 显然，一个零元形成一个子空间，叫做零空间. 除自身及零空间外，不含其他子空间的空间叫做既约空间.

定义 2 假定 $u_1, u_2, \cdots, u_n$ 是 F 的向量空间 V 中元，如果 F 中有 n 个不完全是零的元 $a_1, a_2, \cdots, a_n$ 存在，使

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = 0,$$

那末 $u_1, u_2, \cdots, u_n$ 叫做关于 F **线性相关**；如果象这样的元 $a_1, a_2,$

---

*) 因为 $u = 1 \cdot u + (u - 1 \cdot u)$，命 $1 \cdot u = u'$，$u - 1 \cdot u = u_0$，那末 $u = u' + u_0$. 这时 $1 \cdot u' = u'$，对于 F 中任意元 a，$au_0 = 0$. 我们容易知道，所有的 u'，u_0 分别形成 V 的子空间 V'，V_0，并且 V 是 V'，V_0 的直和(§5.4)，即 $V = V' + V_0$. 因为 F 中任意元零化 V_0，所以在很多场合上讨论 V 时，可以把 V_0 略去，只讨论 V' 就可以. 因此我们常常规定 $1 \cdot u = u$.

$\cdots, a_n$ 不存在，也就是说上面那种关系只有 $a_1, a_2, \cdots, a_n$ 都是零时才成立，那末 $u_1, u_2, \cdots, u_n$ 就叫做关于 F **线性无关**.

F 向量空间中无穷多个元，如果其中某有穷个元关于 F 线性相关，那末它就叫做关于 F **线性相关**；否则，也就是说，如其中任意有穷个元关于 F 都是线性无关，那末它就叫做关于 F **线性无关**.

于是若干个元，如果线性相关，那末它们之间有线性方程的联系，如果线性无关，那末它们之间没有任何线性方程的联系.

以后引用上定义时，如果不引起混淆，为了简便，我们常常把其中"关于 F"略去不写，只说线性相关、线性无关等.

我们很容易知道，V 中一个元 u，如果线性相关，那末 $u=0$，因此 V 中任意非零元线性无关. 在 V 的子集合中，如果其中一部分是线性相关，那末它们全部也线性相关. 假如 V 的子集是线性相关，那末其中至少有一元，譬如 u_n，可以用其中其他有穷个元 $u_1, u_2, \cdots, u_{n-1}$ 的一次式表示，即

$$u_n = a_1u_1 + a_2u_2 + \cdots + a_{n-1}u_{n-1}, \quad a_i \in F,$$

这时，我们又说 u_n 关于 F 是 $u_1, u_2, \cdots, u_{n-1}$ 的**线性组合**，或者说 u_n 关于 F 与 $u_1, u_2, \cdots, u_{n-1}$ **线性相关**. 反过来，假如 n 个元，其中有一元关于 F 是其余元的线性组合，那末它们是线性相关. 因此，若干个元线性相关的必要充分条件是：其中至少有一元是其余有穷个元的线性组合.

定义 3 假定 V 是 F 的向量空间，V 中线性无关元的个数如果有最大数，这最大数，叫做 V 关于 F 的**维数**，用记号 $(V:F)$ 表示. 这时 V 又叫做关于 F 是**有穷维的**，或者简称为是**有穷的**. 如果 V 中线性无关元的个数没有最大数，那末 V 就叫做关于 F 是**无穷维的**，或者简称为**无穷的**. 因为 F 的扩张体 K 是 F 的向量空间，我们把 K 关于 F 的维数，又叫做 K 关于 F 的**次数**.

假定$(V:F)=n$，那末V中有n个元线性无关，并且任意多于n个的元都是线性相关. 如果$u_1, u_2, \cdots, u_n$是V中线性无关的n个元，u是V中任意元，那末u是$u_1, u_2, \cdots, u_n$的线性组合，即

$$u=a_1u_1+a_2u_2+\cdots+a_nu_n, \quad a_i\in F,$$

这表示显然又是一意的.

定义 4 假定$u_1, u_2, \cdots, u_n$是F空间V中元，如果V中任意元u可以用$u_1, u_2, \cdots, u_n$的一次式表示，那末$u_1, u_2, \cdots, u_n$叫做V关于F的**生成元**，V关于F线性无关的生成元，叫做V关于F的**底**.

假如$u_1, u_2, \cdots, u_n$是V关于F的底，我们常常把V写成

$$V=Fu_1+Fu_2+\cdots+Fu_n.$$

这时V中任意元能够一意地表为$u_1, u_2, \cdots, u_n$的线性组合.

譬如复数体是实数体的2维向量空间，$1, i$是它的底. 四元数体是实数体的4维空间，e, i, j, k是它的底. 全矩阵环F_n是体F的n^2维空间，E_{ij}, $i, j=1, 2, \cdots, n$，是它的底，这里E_{ij}是F中i行、j列的元是1(F的单位元)，其他都是零的n级矩阵，多项式环$F[x]$是F的无穷维空间，因为$1, x, \cdots, x^n, \cdots$中任意有穷个元都线性无关.

单扩张体$K=F(\alpha)$，当α是超越元时，它关于F的次数是无穷；当α是n次代数元时，因为$1, \alpha, \cdots, \alpha^{n-1}$是$K$关于$F$的底，所以它的次数是$n$，即$(K:F)=n$.

于是假如$(V:F)=n$，那末V中任意n个线性无关的元都形成它关于F的底，因此有穷维空间都有底. 一般，引用冲恩引理，我们容易证明任意空间都有底[7].

我们知道一个向量空间的底不是唯一的，但是各个底的元数能否一致？如果一致，这个数又等于什么？假如V有由n个元形成的关于F的底，显然$(V:F)\geqslant n$. 如果我们能够证明，这时V中任

意 $n+1$ 个元线性相关，那末 $(V:F)=n$，因此底的元数就是维数了．要证明这个性质，我们需要下面的定理．

定理 1 假定 n 个未定元 $x_1, \cdots, x_n$ 的齐次线方程组

$$\sum_{j=1}^{n} a_{ij}x_j=0, \quad i=1, 2, \cdots, m$$

中系数 a_{ij} 都是体 F 中元，并且 $n>m$，那末在 F 中，这方程组有不完全都是零的解．

证明 我们对 m 用归纳法来证明．

当 $m=1$ 时，定理显然成立．假定 $m-1$ 时定理成立，我们命

$$l_i=\sum_{j=1}^{n} a_{ij}x_j, \quad i=1, 2, \cdots, m.$$

如果所有的 $a_{i1}=0$，定理显然成立．因此我们可以假设 $a_{11}\neq 0$．于是线方程组

$$l_1=0, \quad l_2=0, \quad \cdots, \quad l_m=0$$

的任意解都是线方程组

$$l_1=0, \quad l_2-a_{21}a_{11}^{-1}l_1=0, \quad \cdots, \quad l_m-a_{m1}a_{11}^{-1}l_1=0$$

的解，反过来也成立．但线方程组

$$l_2-a_{21}a_{11}^{-1}l_1=0, \quad \cdots, \quad l_m-a_{m1}a_{11}^{-1}l_1=0$$

只有 $n-1$ 个未定元 $x_2, \cdots, x_n$，方程的个数是 $m-1$，由归纳法的假设，在 F 中，它有不完全是零的解 $x_i=\alpha_i$，$i=2, \cdots, n$．于是

$$x_1=-a_{11}^{-1}(a_{12}\alpha_2+\cdots+a_{1n}\alpha_n), \quad x_2=\alpha_2, \cdots, x_n=\alpha_n,$$

就是 $l_i=0 (i=1, 2, \cdots, m)$ 在 F 中不完全是零的解，因此定理得证．

定理 2 假设 n 个元 $u_1, u_2, \cdots, u_n$ 是 V 关于 F 的底，那末 V 中任意 $n+1$ 个元关于 F 线性相关．

证明 假设 $v_1, v_2, \cdots, v_{n+1}$ 是 V 中任意 $n+1$ 个元，

$$v_i=a_{i1}u_1+a_{i2}u_2+\cdots+a_{in}u_n, \quad i=1, 2, \cdots, n+1.$$

我们的问题是在 F 中能否有不完全为零的 $n+1$ 个元 $b_1, b_2, \cdots, b_{n+1}$，使

$$b_1v_1+b_2v_2+\cdots+b_{n+1}v_{n+1}=0.$$

我们把这式写成

$$\sum_{i=1}^{n+1}b_iv_i=\sum_{i=1}^{n+1}b_i\sum_{j=1}^{n}a_{ij}u_j=\sum_{j=1}^{n}\left(\sum_{i=1}^{n+1}b_ia_{ij}\right)u_j.$$

由定理 1，齐次线方程组

$$\sum_{i=1}^{n+1}x_ia_{ij}=0,\quad j=1, 2, \cdots, n,$$

在 F 中有不完全是零的解，假如我们挑选 $b_1, b_2, \cdots, b_{n+1}$ 就是这不完全是零的解，那末 $\sum_{i=1}^{n+1}b_iv_i=0$，因此 $v_1, v_2, \cdots, v_{n+1}$ 线性相关，所以定理成立.

于是我们有

定理 3 F 的向量空间 V 关于 F 的底的元数等于维数

$$(V:F).$$

下面是关于维数的一个重要关系.

定理 4 假如 V 是体 K 的向量空间，F 是 K 的子体，如果 V 关于 F 是有穷维，那末 V 关于 K 以及 K 关于 F 都是有穷维. 反过来，如果 V 关于 K 是有穷维，K 关于 F 是有穷维，那末 V 关于 F 也是有穷维，并且

$$(V:F)=(V:K)(K:F).$$

证明 假如 V 关于 F 是有穷维，因为 $K\supseteq F$，所以 V 关于 K 也是有穷维. 再假定 u 是 V 中非零元，显然所有形状象 au，$a\in K$ 的元形成 V 的子空间 Ku，因为 V 关于 F 是有穷，所以 Ku 关于 F 也是有穷. 命 $\alpha_1u, \alpha_2u, \cdots, \alpha_mu$ 是 Ku 关于 F 的底，那末

$$au=a_1\alpha_1u+a_2\alpha_2u+\cdots+a_m\alpha_mu,$$

也就是说，

$$(a-(a_1\alpha_1+a_2\alpha_2+\cdots+a_m\alpha_m))u=0,$$

于是

$$a=a_1\alpha_1+a_2\alpha_2+\cdots+a_m\alpha_m.$$

因为 $\alpha_1, \alpha_2, \cdots, \alpha_m$ 显然关于 F 线性无关，所以 $\alpha_1, \alpha_2, \cdots, \alpha_m$ 是 K 关于 F 的底，这就是说，K 关于 F 是有穷的，因此定理的前段成立。下面我们来证明定理的后段。

假如 $(V:K)=n$, $u_1, u_2, \cdots, u_n$ 是 V 关于 K 的底；$(K:F)=m$, $v_1, v_2, \cdots, v_m$ 是 K 关于 F 的底，那末 mn 个元

$$v_iu_j,\quad i=1, 2, \cdots, m;\quad j=1, 2, \cdots, n,$$

是 V 中关于 F 线性无关的元。这是因为，如果

$$\sum_{j=1}^{n}\sum_{i=1}^{m}c_{ij}v_iu_j=\sum_{j=1}^{n}\left(\sum_{i=1}^{m}c_{ij}v_i\right)u_j=0,\quad c_{ij}\in F,$$

因为 $u_1, u_2, \cdots, u_n$ 关于 K 线性无关，所以我们有

$$\sum_{i=1}^{m}c_{ij}v_i=0,\quad j=1, 2, \cdots, n.$$

又因为 $v_1, v_2, \cdots, v_m$ 关于 F 是线性无关，所以

$$c_{ij}=0,\quad i=1, 2, \cdots, m;\ j=1, 2, \cdots, n.$$

再假如 α 是 V 中任意元，因为 u_i 是 V 关于 K 的底，所以

$$\alpha=\sum_{j=1}^{n}a_ju_j,\quad a_j\in K.$$

又因为 v_i 是 K 关于 F 的底，所以

$$a_j=\sum_{i=1}^{m}b_{ij}v_i,$$

因此

$$\alpha=\sum_{j=1}^{n}\sum_{i=1}^{m}b_{ij}v_iu_j.$$

这就是说，V 中任意元是 v_iu_j 的线性组合，因此 v_iu_j 是 V 关于 F 的底，所以 $(V:F)=mn$。于是定理的后段成立，因此定理成立。

假如 $(V:F)=1$, 并且 $V\supseteq F$, 那末 $V=F$。这是因为，V 中任意非零的元都是 V 关于 F 的底，因此如果我们取 F 的单位元 e

做底，那末$V=F\cdot e=F$．于是由上面定理我们又得知，假如$V\supseteq K\supseteq F$，如果$(V:F)=(K:F)$，那末$(V:K)=1$，因此$V=K$．如果$(V:F)=(V:K)$，那末$(K:F)=1$，因此$K=F$．

我们知道F的代数单扩张体$F(\alpha)$与$F(\beta)$关于F是同值时，α,β不一定是$F[x]$中同一既约多项式的零点，假如α在$F(\beta)$的象是α'，那末$F(\alpha)\cong F(\alpha')$，于是$(F(\alpha'):F)=(F(\beta):F)$，但$F(\alpha')\subseteq F(\beta)$，所以$F(\alpha')=F(\beta)$．这就是说，$F(\beta)$有这样的本原元$\alpha'$，它是$F[x]$中$\alpha$所适合的既约多项式的零点．

在定义1中，F中元a与V中元u的乘积我们是把a写在u的左边，所以这时我们又叫V做F的左向量空间．假如我们把F中元写在V中元的右边，我们就叫V做F的**右向量空间**，这时上面的结果都能够同样证明一一成立．

上面是介绍向量空间的基本概念和性质，很多是在线代数中我们所熟悉的，下面我们来介绍代数，它是特殊的向量空间．

假定可换体F的n维向量空间A是环，并且

(1) $$a(uv)=(au)v=u(av),\quad a\in F,\quad u,v\in A,$$

那末A叫做F的n**次代数**，或简单地叫做**代数**，F叫做A的**基础体**．代数是体时又叫做**可除代数**．

譬如高斯数体是有理数体的2次可除代数，复数体是实数的2次可除代数，四元数体是实数体的4次可除代数．假如群G的元数是n，那末群环$F(G)$是可换体F的n次代数，全矩阵环F_n是F的n^2次代数．任一体如果关于包含在它中心的子体F是有穷的，那末它就是F的可除代数．

要注意的是，代数不一定包含它的基础体，也就是说，F的代数A不一定包含F．假如A包含F，那末F包含在A的中心里面．假定A有单位元e，显然A中所有形状象ae，$a\in F$的元形成的子体Fe与F同构，因此由§3.3的挖补定理，我们可以把F

看成 A 的子体．这就是说，有单位元的代数包含它的基础体，所以可除代数包含它的基础体．

假定 $A=Fu_1+Fu_2+\cdots+Fu_n$ 是 F 的 n 次代数，由(1)，我们有

$$(au)(bv)=(ab)uv,$$

于是

$$\left(\sum_{i=1}^{n}a_iu_i\right)\left(\sum_{j=1}^{n}b_ju_j\right)=\sum_{i,j=1}^{n}a_ib_j(u_iu_j). \tag{2}$$

命

$$u_iu_j=\sum_{r=1}^{n}c_{ij}^{(r)}u_r,\quad c_{ij}^{(r)}\in F, \tag{3}$$

因为

$$u_i(u_ju_k)=\sum_{s=1}^{n}c_{jk}^{(s)}u_iu_s=\sum_{t=1}^{n}\left(\sum_{s=1}^{n}c_{jk}^{(s)}c_{is}^{(t)}\right)u_t,$$

$$(u_iu_j)u_k=\sum_{t=1}^{n}\left(\sum_{s=1}^{n}c_{ij}^{(s)}c_{sk}^{(t)}\right)u_t,$$

所以

$$\sum_{s=1}^{n}c_{ij}^{(s)}c_{sk}^{(t)}=\sum_{s=1}^{n}c_{jk}^{(s)}c_{is}^{(t)},\quad i,\ j,\ k,\ t=1,\ 2,\ \cdots,\ n. \tag{4}$$

反过来，假如向量空间 $A=Fu_1+Fu_2+\cdots+Fu_n$，其中任意两元 $\sum a_iu_i$, $\sum b_ju_j$ 的乘积是由(2)式来规定，并且表示 u_iu_j 的(3)式中 $c_{ij}^{(r)}$ 又适合(4)式，我们容易证明 A 是 F 的代数．

于是代数 A 的构造由 F 中适合(4)式的 n^3 个元 $c_{ij}^{(r)}$ 一意决定，所以 $c_{ij}^{(r)}$ 又叫做 A 的**构造元素**．

假定 A 是 F 的代数，如果 B 是 A 的子环，并且又是 F 的代数，那末 B 叫做 A 的**子代数**．代数 A 的子代数如果又是把 A 看成环时的理想子环，就叫做代数 A 的理想子环．显然代数 A 的理想子环与把 A 只看成环时的理想子环是有区别的，前者还要求它是子空间，在 A 有单位元时，两者是一致的．

一个已知可换体的代数如何决定，也就是说它的构造如何，是

代数的主要问题之一．显然复数体的可除代数仍然是复数体．下面我们来讨论实数体的可除代数的构造．

我们知道，实数体、复数体及四元数体分别是实数体的 1 次、2 次及 4 次可除代数，因此我们要反问，实数体的可除代数是否只有这三类？1877 年弗罗宾纽斯解答了这问题．下面就是著名的弗罗宾纽斯定理．

定理 5　实数体的可除代数只有实数体、复数体及四元数体三类．

证明　假设 F 是实数体，K 是 F 的 n 次可除代数，如果 $n=1$，那末 $K=F$．也就是说，这时 K 是实数体．

如果 $n>1$，那末 K 中有不是实数的数 α，这 α 当然是 F 的代数元．因为 $F[x]$ 中既约多项式的次数是 1 或 2，而 α 不在 F 中，所以 $F[x]$ 中 α 所适合的既约多项式的次数是 2．我们假定这既约多项式是

$$x^2+px+q=0,\quad p,\ q \text{ 都是实数，}$$

因为它没有实根，所以 $q-\frac{p^2}{4}>0$，命

$$q-\frac{p^2}{4}=r^2,\quad r \text{ 是实数，}$$

那末 K 中元

$$i=\frac{1}{r}\left(\alpha+\frac{p}{2}\right)$$

有 $i^2=-1$，即 i 满足既约方程 $x^2=-1$．于是 $F(i)$ 是 F 的 2 次体．如果 $n=2$，那末 $K=F(i)$，因为 $F(i)$ 显然与复数体同构，所以这时 K 是复数体．

如果 $n>2$，我们来证明 K 中包含有四元数体．因为这时 K 中除 $F(i)$ 外还有元素，同上面一样，假定 j_0 是其中一元，那末 $j_0^2=-1$．下面我们来计算 ij_0 及 j_0i．因为 K 中任意元是 $F[x]$ 中 2 次多项式的零点，当然 $i+j_0$，$i-j_0$ 也是如此．于是我们有

$$(5)\qquad \begin{cases}(i+j_0)^2=-2+ij_0+j_0i=a(i+j_0)+b,\\(i-j_0)^2=-2-ij_0-j_0i=c(i-j_0)+d,\end{cases}$$

这里 a, b, c, d 都是实数，将上面两式相加，即得

$$-4=(a+c)i+(a-c)j_0+(b+d).$$

因为 j_0 不在 $F(i)$ 中，所以 1, i, j_0 关于 F 线性无关，因此

$$a+c=0,\quad a-c=0.$$

于是 $a=0$, $c=0$. 因此由(5)中第一式即得

$$(6)\qquad ij_0+j_0i=2t,\quad t=\frac{1}{2}(b+2).$$

再根据(6)式，我们来求四元数体中的 j. 命 $j'=j_0+ti$, 我们就有

$$ij'+j'i=i(j_0+ti)+(j_0+ti)i=ij_0+j_0i-2t=0,$$

但 $$j'^2=-1+t(ij_0+j_0i)-t^2=-1+t^2$$

必须是一个负数，即 $j'^2<0$，因为不如此，j' 是实数，那末 1, i, j_0 就线性相关，这与假设不合. 命 $j'^2=-s^2$, s 是实数，就有 $j=\frac{1}{s}j'$，这时，

$$j^2=-1,$$

并且 $ij+ji=\frac{1}{s}(ij'+j'i)=0$, 即 $ij=-ji$. 设 $k=ij$, 得 $ij=-ji=k$, 再由计算容易得知

$$k^2=-1,\quad ki=-ik=j,\quad jk=-kj=i.$$

又 1, i, j, k 线性无关，这是因为，如果

$$k=a+bi+cj,\quad a,\ b,\ c \text{ 是实数},$$

用 i 左乘，即得

$$\begin{aligned}-j&=ai-b+ck=ai-b+c(a+bi+cj)\\&=ca-b+(a+bc)i+c^2j.\end{aligned}$$

因为 $1, i, j$ 线性无关，所以 $c^2=-1$，这与 c 是实数的假设不合，因此 K 含有由所有四元数 $a+bi+cj+dk$, $a, b, c, d\in F$，形成的四元数体做它的子体，如果 $n=4$，那末 K 就是四元数体.

最后我们来证明 $n\leqslant 4$. 假如 $n>4$，那末 K 中又有元 $l^2=-1$，并且它与 $1, i, j, k$ 线性无关. 同(6)式一样，我们有

$$il+li=a,\quad jl+lj=b,\quad kl+lk=c,\quad a, b, c \text{ 是实数},$$

于是
$$lk=(li)j=aj-ilj=aj-i(b-jl)=aj-bi+ijl$$
$$=aj-bi+kl=aj-bi+c-lk,$$

因此

$$aj-bi+c=2lk.$$

用 k 右乘，即得

$$ai+bj+ck=-2l,$$

这与 i, j, k, l 线性无关的假设不合，所以 n 不能大于 4. 于是定理得证.

此外，1932 年亚尔伯脱 (A. A. Albert, 1905～) 及哈综 (H. Hasse, 1898～) 曾证明[8]，关于代数体的可除代数是正规可除代数*). 再 1933 年曾炯之 (1896～1940) 曾经证明，函数体 $\Omega(x)$ 的可除代数只有 $\Omega(x)$ 自身[9]. 这些都是有价值的构造定理.

假如 F 是可换体，$u_1, u_2, \cdots, u_n$ 是适合条件

$$u_i^2=1,\quad u_iu_j=-u_ju_i,\quad i\neq j$$

的元，由 § 3.5 我们把 $u_1, u_2, \cdots, u_n$ 陆续添加于 F 所得到的 F 扩张环 $F[u_1][u_2]\cdots[u_n]$ 是 F 的代数，叫做**克里福德** (W. K. Clifford, 1845～1879) **代数**. 显然，2^n 个元 $1, u_i, u_iu_j, \cdots, u_1u_2\cdots u_n$ 是它的

---

*) 假如 A 是可换体 F 的代数，e 是它的单位元，如果 A 的中心是 Fe，也就是说，如果 F 是 A 的中心，那末 A 叫做 F 的**正规代数**. 正规代数是可除代数时，叫做**正规可除代数**. 因此四元数体是实数体的正规可除代数.

底．关于这类代数，李华宗(1911～1949)曾做过比较全面的研究[10]．

在代数中，假如把它的乘法结合律这个条件挖去，那末它就叫做**非结合代数**．因此非结合代数虽然对乘法也是闭合的，但不再是环了．与这相应，上面我们介绍的代数，因为它满足乘法结合律，所以我们又常常叫它做**结合代数**．

假定 A 是非结合代数，对于 A 中任意元 a, b, c，如果

$$ab=ba,\quad (a^2b)a=a^2(ba),$$

那末 A 叫做**约当**(C. Jordan, 1838～1922)**代数**；如果

$$ab=-ba,\quad a(bc)+b(ca)+c(ab)=0,$$

那末 A 叫做**李**(M. S. Lie, 1842～1899)**代数**．这些都是在非结合代数中，目前性质知道得比较多的代数[11]．

习 题 4.4

1．假设 $K\supseteq L\supseteq F$，K 是 F 的有穷次体，试证 $(L:F)$ 是 $(K:F)$ 的因数．

2．假设 Q 是有理数体，试求 $Q(i, \sqrt{2})$ 关于 Q 的次数．

3．假如 K 是 F 的有穷次体，试证 K 中任意元关于 F 的次数是 $(K:F)$ 的因数．

4．假如 F 是特征数为 p 的质体，K 是 F 的 n 次体，试求 K 的元数．

5．试证 $E_{ij}(i, j=1, 2, \cdots, n)$ 是全矩阵环 F_n 关于 F 的底．

6．假定 K 是有理数体 Q 的 2 次代数体，试证 $K=Q(\sqrt{a})$，这里 a 是没有相同的质因数的整数．并且当 $a\neq b$ 时，$Q(\sqrt{a})\neq Q(\sqrt{b})$．

7．试证 F 的代数的中心仍然是 F 的代数．

8．代数是可除代数的必要充分条件是它是无零因子环．

9．试用 §3.4 习题 3 证明：任意没有单位元的代数能够嵌入于有单位元的代数．

10．假定 A 是结合代数．其中任意两元 a, b 的乘积 ab 如果用 $a\circ b=ab+ba$ 代替，那末 A 是约当代数，如果 A 对乘法不是可换，ab 用 $a\times b=ab-ba$ 代替，那末 A 就是李代数．

§4.5 代数扩张体

前面介绍了扩张体的基本概念及基本性质，并且讨论了单扩张体的构造．此后各节是讨论一般扩张体的构造，主要是代数扩张体的构造．

假如 K 是 F 的扩张体，$(K:F)=n$，α 是 K 中任意元，那末 $n+1$ 个元

$$1,\ \alpha,\ \cdots,\ \alpha^n$$

线性相关，因此

$$c_0+c_1\alpha+\cdots+c_n\alpha^n=0,$$

所以 α 是多项式

$$f(x)=c_0+c_1x+\cdots+c_nx^n$$

的零点．这就是说，K 中任意元都是 F 的代数元．象这样的 F 扩张体，其中任意元都是 F 的代数元时，叫做 F 的**代数扩张体**或 F 的**代数体**．F 的扩张体如果不是代数扩张体，就叫做 F 的**超越扩张体**，或 F 的**超越体**．

譬如复数体是实数体的代数体，实数体是有理数体的超越体．体 F 的超越单扩张体是 F 的超越体．

根据上面的讨论，我们有

定理 1 可换体 F 的有穷次扩张体是 F 的代数体．

于是 F 的代数单扩张体 $F(\alpha)$ 是 F 的代数扩张体．一般，假如 $\alpha_1,\ \cdots,\ \alpha_n$ 都是 F 的代数元，因为 F 的代数元也是 F 的扩张体的代数元，由 §4.4 定理 4，我们不难得知可换体 $F(\alpha_1,\ \cdots,\ \alpha_n)$ 是 F 的有穷次体，因此它是 F 的代数体，所以在 F 的可换扩张体中，F 的代数元的和、差、积、商仍然是 F 的代数元．

要注意的是，上定理的逆不成立，即 F 的代数体不一定是 F 的有穷次体．譬如所有代数数形成的体是有理数体 Q 的代数体，显然它不是 Q 的有穷次体．

假定 L 是体 K、F 的中间体，即 $K \supseteq L \supseteq F$，如果 K 是 F 的代数体，显然 K 是 L 的代数体，L 是 F 的代数体．下面就是它的逆．

定理 2 假定可换体 K 是 L 的代数体，L 是 F 的代数体，那末 K 是 F 的代数体．这就是说，在可换体中代数体这个性质是适合传递律的．

证明 假定 α 是 K 中元，$\alpha_0, \alpha_1, \cdots, \alpha_n$ 是 $L[x]$ 中 α 适合的既约多项式的系数，因为 L 是 F 的代数元，所以 α_i 是 F 的代数元．由 §4.4 定理 4，$L' = F(\alpha_0, \alpha_1, \cdots, \alpha_n)$ 是 F 的有穷次体，于是 α 是 F 的代数元，因此定理成立．

假定可换体 K 是 F 的扩张体，那末 K 中所有 F 的代数元形成一子体，我们用 L 来表示．显然，它是 K、F 的中间体．并且是 K 中 F 的**最大代数体**．这时 K 中除 L 的元外，任意元都是 L 的超越元．这是因为，假如 α 是 K 中 L 的代数元，那末 $L(\alpha)$ 是 L 的代数扩张体．因为 L 是 F 的代数扩张体，所以 $L(\alpha)$ 也是 F 的代数扩张体，于是 α 是 F 的代数元，因此 $\alpha \in K$．象这样的 L 扩张体，其中除 L 中元外，任意元都是 L 的超越元时，叫做 L 的**纯超越扩张体**，或者叫做 F 的**纯超越体**．因此可换体 K 可以先从 F 代数扩张到 L，再从 L 纯超越扩张而成．也就是说，任意扩张可以由先代数扩张再超越扩张而成．

习 题 4.5

1．若无零因子环 R 中任意元是它的子体 F 的代数元，试证 R 是 F 的代数体．

§ 4.6 分裂体，正规扩张体

我们知道，可换体 F 的代数体 K 中元都是 $F[x]$ 中多项式的零点，所以 K 的某些性质可以由 $F[x]$ 中多项式的性质来确定，因此在讨论 K 时，我们可以从 $F[x]$ 中多项式入手. 这节我们讨论 F 的两个特殊的代数扩张体，下节根据 $F[x]$ 中多项式零点的性质把 F 的代数体来分类.

由 § 4.3 我们知道，$F[x]$ 中任意多项式 $f(x)$ 在 F 的某扩张体 K 中有它的零点存在，因此在 K 中 $f(x)$ 有一次因式. 这时我们也说它在 K 中能够分裂. 假如 $f(x)$ 在 K 中能够分裂为一次因式的乘积，我们就说它在 K 中能够完全分裂. 譬如系数是复数的多项式在复数体中就能够完全分裂.

定义 1 假设 $f(x)$ 是 $F[x]$ 中多项式，可换体 K 是 F 的扩体，如果在 K 中，$f(x)$ 能够完全分裂，即

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\quad \alpha_i\in K,$$

但在 K、F 的任意异于 K 的中间体中(假如存在)，$f(x)$ 不能够完全分裂，那末 K 叫做 $f(x)$ 的**分裂体**.

譬如 Q 是有理数体，$f(x)=x^2-2$，因为在 $Q(\sqrt{2})$ 中，

$$f(x)=(x-\sqrt{2})(x+\sqrt{2}),$$

并且此时 $Q(\sqrt{2})$，Q 没有异于 $Q(\sqrt{2})$ 的中间体，所以 $Q(\sqrt{2})$ 是 $f(x)=x^2-2$ 的分裂体.

假如可换体 K 是 $F[x]$ 中 $f(x)$ 的分裂体，那末 K 就是由 F 添加 $f(x)$ 在 K 中所有零点形成的体. 因此 K 是 F 的有穷次代数体.

定理 1 $F[x]$ 中任意多项式 $f(x)$ 有分裂体.

证明 假设 $f(x)$ 在 $F[x]$ 中分裂为既约多项式 $f_i(x)$ 的乘积，

即

$$f(x)=f_1(x)f_2(x)\cdots f_{m_1}(x),$$

如果 $f_i(x)$ 都是 1 次，那末 F 就是 $f(x)$ 的分裂体．如果 $f_i(x)$ 的次数不都是 1，假如 $f_1(x)$ 的次数大于 1，我们把 $f_1(x)$ 的一零点 α_1 添加于 F 得到 $F_1=F(\alpha_1)$，在 $F_1[x]$ 中，$f(x)$ 最少有一个 1 次因式 $x-\alpha_1$，因此 $f(x)$ 能够分裂为 1 次因式 $x-\alpha_1$ 及既约因式 $g_i(x)$ 的乘积，即

$$f(x)=(x-\alpha_1)g_1(x)\cdots g_{m_1}(x).$$

如果 $g_i(x)$ 都是 1 次，那末 F_1 就是 $f(x)$ 的分裂体；如果 $g_i(x)$ 不都是 1 次，重复引用上面的方法，因为 $f(x)$ 的次数是有穷，所以在 F 的扩张体中，$f(x)$ 的 1 次因式只能有穷多个，因此继续添加有穷个零点 α_i 后，我们得到体 $F_m=F(\alpha_1,\ \cdots,\ \alpha_m)$．在 F_m 中，$f(x)$ 能够完全分裂，因此定理得证．

由上面的证明及 §4.3，我们不难知道任意多项式的分裂体不是唯一的．为了更好地说明它们之间的关系，我们先介绍下面一个基本概念．

定义 2 假如体 K，$\overline{K}$ 分别是体 F，$\overline{F}$ 的扩张体，σ 是 F，$\overline{F}$ 的同构，τ 是 K，$\overline{K}$ 的同构，如果

$$\tau(a)=\sigma(a),\quad a\in F,$$

也就是说，F 中任意元对于 σ，τ 的象都相同，那末 τ 叫做 σ 的**延长**，而 K，$\overline{K}$ 叫做 F，$\overline{F}$ 的**延长**．

当 $F=\overline{F}$，σ 是恒等映射时，τ 就是 K，$\overline{K}$ 关于 F 的同值，因此同值是延长的特例．

引用延长这个概念，我们得到下面比 §4.3 定理 3 更广泛的定理．

定理 2 假如体 F，$\overline{F}$ 同构，$g(x)$ 是 $F[x]$ 中既约多项式，$\overline{g}(x)$ 是 $\overline{F}[x]$ 中与 $g(x)$ 对应的多项式（即系数分别是 $g(x)$ 中系数的

象)，α 是 $g(x)$ 在 F 的扩张体中的零点，$\bar{\alpha}$ 是 $\bar{g}(x)$ 在 $\bar{F}$ 的扩张体中的零点，那末 $F(\alpha)$，$\bar{F}(\bar{\alpha})$ 是 F，$\bar{F}$ 的延长.

证明　首先 $\bar{g}(x)$ 是 $\bar{F}[x]$ 中既约多项式. 这是因为，如果在 $\bar{F}[x]$ 中，$\bar{g}(x)$ 是可约的，$\bar{g}(x)=\bar{g}_1(x)\bar{g}_2(x)$，假定 $g_1(x)$，$g_2(x)$ 是 $F[x]$ 中分别与 $\bar{g}_1(x)$，$\bar{g}_2(x)$ 对应的多项式，因为 $F\cong\bar{F}$，对于 $\bar{F}$ 中任意两元的和及积的象源分别是它们的象源的和及积，所以 $g(x)=g_1(x)g_2(x)$，这与 $g(x)$ 是既约的假设不合.

再假设 F，$\bar{F}$ 的同构把 F 中元 a 变成 $\bar{F}$ 中元 $\bar{a}$，$g(x)$ 的次数是 n，那末 $F(\alpha)$ 中任意元可以写成 $\sum\limits_{i=0}^{n-1}a_i\alpha^i$，$\bar{F}(\bar{\alpha})$ 中任意元可以写成 $\sum\limits_{i=0}^{n-1}\bar{a}_i\bar{\alpha}^i$，因此下面的对应 σ：

$$f(\alpha)=\sum_{i=0}^{n-1}a_i\alpha^i\rightarrow\overline{f(\alpha)}=\sum_{i=0}^{n-1}\bar{a}_i\bar{\alpha}^i$$

显然是 $F(\alpha)$ 射到 $\bar{F}(\bar{\alpha})$ 上的映射，并且还是可逆的. 如果我们能够证明 σ 是 $F(\alpha)$ 射到 $\bar{F}(\bar{\alpha})$ 上的同构，因为 $\sigma(a)=\bar{a}$，$a\in F$，于是 $F(\alpha)$，$\bar{F}(\bar{\alpha})$ 是 F，$\bar{F}$ 的延长，因此定理就告成立.

假定 $h(\alpha)=\sum\limits_{i=0}^{n-1}b_i\alpha^i$，因为

$$f(\alpha)+h(\alpha)=\sum_{i=0}^{n-1}(a_i+b_i)\alpha^i,\quad \overline{a_i+b_i}=\bar{a}_i+\bar{b}_i,$$

所以
$$\overline{f(\alpha)+h(\alpha)}=\overline{f(\alpha)}+\overline{h(\alpha)}.$$

命
$$f(x)h(x)=q(x)g(x)+r(x),$$

因为对于 F 中任意元 a，b，我们有 $\overline{a+b}=\bar{a}+\bar{b}$，$\overline{ab}=\bar{a}\bar{b}$，因此

$$\bar{f}(x)\bar{h}(x)=\bar{q}(x)\bar{g}(x)+\bar{r}(x),$$

于是
$$f(\alpha)h(\alpha)=r(\alpha),\quad \bar{f}(\bar{\alpha})\bar{h}(\bar{\alpha})=\bar{r}(\bar{\alpha}),$$

所以
$$\overline{f(\alpha)h(\alpha)}=\overline{f(\alpha)}\cdot\overline{h(\alpha)}.$$

这就是说，映射 σ 是 $F(\alpha)$ 射到 $\bar{F}(\bar{\alpha})$ 上的同构，因此 $F(\alpha)$，$\bar{F}(\bar{\alpha})$ 是 F，$\bar{F}$ 的延长，所以定理成立.

现在来讨论分裂体间的关系.

定理 3 假设 F 是可换体，$f(x)$ 是 $F[x]$ 中多项式，K，$\overline{K}$ 是 $f(x)$ 的分裂体，那末 K，$\overline{K}$ 关于 F 同值，也就是说，任意多项式的分裂体除同值的外是唯一的.

证明 我们先给出 $f(x)$ 的零点与它的既约因式的关系.

假如 $g(x)$ 是 $f(x)$ 在 $F[x]$ 中的既约因式，$f(x)=q(x)g(x)$，因为 $f(x)$ 在 K 中完全分裂，即

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

所以 $$q(x)g(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

假如 α 是 $g(x)$ 的零点，那末在单扩张 $K(\alpha)$ 中，

$$(\alpha-\alpha_1)(\alpha-\alpha_2)\cdots(\alpha-\alpha_n)=q(\alpha)g(\alpha)=0.$$

因为 $\alpha-\alpha_i$ 是体 $K(\alpha)$ 中元，所以在 $\alpha-\alpha_i$ 中必有是零元的，譬如说 $\alpha-\alpha_1=0$，我们就有 $\alpha=\alpha_1$. 这就是说，$f(x)$ 的分裂体包含它的既约因式 $g(x)$ 的分裂体.

现在我们来证明本定理.

假设 $f(x)$ 在 F 中分裂为既约多项式 $f_i(x)$ 的乘积，即

$$f(x)=f_1(x)f_2(x)\cdots f_m(x),$$

假如 $f_i(x)$ 都是 1 次的，那末 F 就是 $f(x)$ 的分裂体，因此这时定理成立. 假如 $f_i(x)$ 不都是 1 次，$f_1(x)$ 的次数大于 1，我们命 α_1，$\overline{\alpha}_1$ 分别是 K，$\overline{K}$ 中 $f_1(x)$ 的零点，由定理 2，$F(\alpha_1)$，$F(\overline{\alpha}_1)$ 关于 F 同值. 假如 $F(\alpha_1)$ 是 $f(x)$ 的分裂体，那末 $F(\overline{\alpha}_1)$ 也就是 $\overline{f}(x)$ 的分裂体. 因此这时定理成立. 假如 $F(\alpha_1)$ 不是 $f(x)$ 的分裂体，在 $F(\alpha_1)$ 中再将 $f(x)$ 分解为既约多项式的乘积，重复引用上面的方法，因为 $f(x)$ 的次数是有穷，而 K 是由 F 添加 $f(x)$ 在 K 中所有零点扩张的体，因此继续进行有穷回后，就得到 K，$\overline{K}$，显然它们关于 F 同值，所以定理得证.

由上面的证明我们又知道，假如 $K=F(\alpha_1, \alpha_2, \cdots, \alpha_n)$，那末

$\overline{K}=F(\overline{\alpha}_1, \overline{\alpha}_2, \cdots, \overline{\alpha}_n)$，并且 K，$\overline{K}$ 有把 α_i 变成 $\overline{\alpha}_i$ 关于 F 的同值.

假如 $F[x]$ 中多项式 $f(x)$ 的分裂体 $K=F(\alpha_1, \cdots, \alpha_n)$ 及 $\overline{K}=F(\overline{\alpha}_1, \cdots, \overline{\alpha}_n)$ 在同一包含体中，那末 K，$\overline{K}$ 不只关于 F 是同值，而且是相等，这是因为在这包含体中，

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_n)=(x-\overline{\alpha}_1)\cdots(x-\overline{\alpha}_n),$$

根据 §3.9 定理 7，这两种分解除顺序外是一致的，因此 K，$\overline{K}$ 是由相同的元添加于 F 扩张的体，所以 $K=\overline{K}$.

由定理 3 的证明，我们还可以知道多项式在一分裂体中如果有 m 重零点，那末在任一分裂体中也同样有 m 重零点，零点的相重数与分裂体的选择无关.

上面我们介绍了分裂体，现在我们来介绍另一类叫做正规体的代数扩张体.

我们知道在 $f(x)$ 的分裂体中，$f(x)$ 当然能够完全分裂，此外还有哪些多项式也能够在其中完全分裂?

假定 $K=F(\alpha_1, \cdots, \alpha_n)$ 是 $F[x]$ 中多项式 $f(x)$ 的分裂体，α_i 是 $f(x)$ 的零点，$g(x)$ 是 $F[x]$ 中的既约多项式，它有一零点 $\beta\in K$，如果 β' 是 $g(x)$ 在 K 的扩张体中任意零点，下面我们来证明 $\beta'\in K$，因此 $g(x)$ 在 K 中也能够完全分裂.

我们知道 $F(\beta)$，$F(\beta')$ 关于 F 同值，并且有不使 F 中任意元变动而把 β 变为 β' 的同值映射. 假如我们把 $f(x)$ 分别看成为 $F(\beta)[x]$，$F(\beta')[x]$ 中多项式，于 $F(\beta)$，$F(\beta')$ 各添加 $f(x)$ 的零点 $\alpha_1, \cdots, \alpha_n$. 一再引用定理 2，就容易得知 $F(\beta)(\alpha_1, \cdots, \alpha_n)$，$F(\beta')(\alpha_1, \cdots, \alpha_n)$ 是 $F(\beta)$，$F(\beta')$ 的延长，并且这延长把 α_i 又变为 α_j，只是它们间的顺序可能有所不同. 因为 K 是 F 的代数体，而 β 是 K 中元，所以 β 是系数为 F 中元的 $\alpha_1, \cdots, \alpha_n$ 的多项式

$$\beta=h(\alpha_1, \cdots, \alpha_n).$$

由 $F(\beta)$，$F(\beta')$ 的同构关系得知 β' 也是系数为 F 中元的 $\alpha_1, \cdots,$

α_n的多项式，因此$\beta'\in F(\alpha_1, \cdots, \alpha_n)$，所以$g(x)$在$K$中完全分裂，这就是说，假如既约多项式$g(x)$在$f(x)$的分裂体能够分裂，那末它在$K$中能够完全分裂。

上面是分裂体的一个性质，F的任意代数体不一定都有这性质。一般来说，我们有

定义 3 假定K是F的可换代数体，并且$F[x]$中任意既约多项式，如果在K中能够分裂，它在K中就能够完全分裂，那末K叫做F的**正规扩张体**，或简称F的**正规体**，有时又叫做F的**伽罗瓦体**。

于是我们得知，F的代数体K中任意元关于F的共轭元如果仍在K中，那末K就是F的正规体，这与§2.4中，群G的子群H中任意元的共轭元仍在H中时，H是G的正规子群的性质一致，但要注意的是，这时K是F的扩张体，而H却是G的子群。

引用上面定义，由前面的讨论，我们有

定理 4 多项式环$F[x]$中任意多项式$f(x)$的分裂体是F的有穷次正规体。

因为F的代数体关于F不一定是有穷的，所以F的正规体关于F也不一定是有穷次的，譬如上节中所有代数形成的体是有理数体Q的正规体，它关于Q不是有穷次。在有穷次时，上面定理的逆定理也是成立的。

定理 5 假如K是F的有穷次正规体，那末K是$F[x]$中某多项式的分裂体。

证明 因为K关于F是有穷次的，所以K是添加其中有穷个元$\alpha_1, \cdots, \alpha_n$于$F$所成的体，即

$$K=F(\alpha_1, \cdots, \alpha_n).$$

假设$f_i(x)$是$F[x]$中零点为α_i的既约多项式，因为K是F的正

规体，所以 $f_i(x)$ 在 K 中完全分裂．于是 $f(x)=\prod_{i=1}^{n}f_i(x)$ 在 K 中也能够完全分裂，因此 K 是 $f(x)$ 的分裂体，所以定理得证．

显然 F 的有穷次扩张体 K 不一定是 F 的正规体．但是由上面的证明，我们可以再扩张 K 使它成为 F 的正规体．也就是说，在 F 的扩张体中有包含 K 的正规体．

添加 $F[x]$ 的既约多项式 $g(x)$ 的一个零点 α 于 F 得到的体 $F(\alpha)$ 一般不一定是 $g(x)$ 的分裂体，因此也不一定是 F 的正规体．如果 $F(\alpha)$ 是 F 的正规扩张体，这时多项式 $g(x)$ 叫做 F 的**正规式**或者叫做**伽罗瓦式**．

下面我们来介绍正规扩张体的一些基本性质，这些性质与 § 2.4 中关于正规子群的非常类似．

由 § 2.4 我们得知，H 是群 G 的正规子群的必要充分条件是 H 与它的共轭子群相等，与这类似，我们有

定理 6 假如 α 是 $F[x]$ 中既约多项式 $g(x)$ 在它的分裂体 K 的零点，α_i 是 K 中 $g(x)$ 的任意零点，那末体 $F(\alpha)$ 是 F 的正规体的必要充分条件是 $F(\alpha)$ 与它关于 F 的任意共轭体 $F(\alpha_i)$ 相等，即

$$F(\alpha)=F(\alpha_i).$$

证明 假如 $F(\alpha)$ 是 F 的正规体，因为 α_i 是 $g(x)$ 的零点，所以 $\alpha_i\in F(\alpha)$，因此 $F(\alpha_i)\subseteq F(\alpha)$，但 $(F(\alpha):F)=(F(\alpha_i):F)$，所以 $(F(\alpha):F(\alpha_i))=1$，于是 $F(\alpha_i)=F(\alpha)$．反过来，假如 $F(\alpha_i)=F(\alpha)$，那末 $F(\alpha)$ 就是 $g(x)$ 的分裂体，所以 $F(\alpha)$ 是 F 的正规体，因此定理成立．

我们知道，假如 H，K 都是群 G 的子群，并且 $G\supseteq K\supseteq H$，如果 H 是 G 的正规子群，那末 H 也是 K 的正规子群．与这类似，我们有

定理 7 假定 $K\supseteq L\supseteq F$，并且 K 是 F 的正规体，那末 K 也是 L 的正规体．

证明　因为 K 是 F 的正规体，所以 K 是 F 的代数体，因此 K 也是 L 的代数体．再假如 $g(x)$ 是 $L[x]$ 中既约多项式，α 是它在 K 中一零点，$h(x)$ 是 $F[x]$ 中零点为 α 的既约多项式，由§4.3 习题 6，我们得知 $g(x)$ 是 $h(x)$ 的因式．因为 $h(x)$ 在 K 中能够完全分裂，所以 $g(x)$ 在 K 中也能够完全分裂，因此 K 是 L 的正规体，于是定理成立．

同群的情况一样，要注意的是，在上面定理中，虽然 K 是 F 的正规体，但 L 不一定是 F 的正规体．譬如 Q 是有理数体，ω 是 1 的虚立方根，那末

$$Q(\sqrt[3]{2},\omega)\supset Q(\omega\sqrt[3]{2})\supset Q,$$

这时 $Q(\sqrt[3]{2},\omega)$ 是多项式 x^3-2 的分裂体，所以它是 Q 的正规体，但 $Q(\omega\sqrt[3]{2})$ 不是 Q 的正规体．

此外，还要注意的是，如果 K 是 L 的正规体，L 是 F 的正规体，那末 K 也不一定是 F 的正规体．这就是说，正规体这个关系是不适合传递律的．譬如 Q 是有理数体，因为

$$Q(\sqrt[4]{2})\supset Q(\sqrt{2})\supset Q,$$

显然 $Q(\sqrt[4]{2})$ 是 $Q(\sqrt{2})$ 的正规体，$Q(\sqrt{2})$ 是 Q 的正规体，但 $Q(\sqrt[4]{2})$ 不是 Q 的正规体．

习　题　4.6

1．试求多项式 x^3-x^2-x-2 关于有理数体的分裂体．

2．试证多项式 x^4+4x^2+2 是有理数体的正规式．

3．试证 F 的 2 次体是 F 的正规体．

4．试证 $F[x]$ 中 n 次多项式的分裂体关于 F 的次数不能大于 $n!$．

5．假如把 $F[x]$ 中无穷多个多项式的零点都添加于 F，得到的体也是 F 的正规体，如何证明？

6．试证整系数 3 次多项式成为有理数体的正规式的必要充分条件是，它的判别式是有理数的平方．

§ 4.7 可离扩张体，不可离扩张体

代数扩张体与它所添加的代数元有关，而代数元又与它所适合的既约多项式有关，但既约多项式有的有重零点，有的没有重零点，这节我们就这两种情形来讨论代数扩张体的构造。

我们知道，在普通代数中既约多项式是没有重零点的，现在要问，如果 F 是任意可换体，$F[x]$ 中既约多项式 $f(x)$ 是否有重零点？因为多项式零点的重数与它的分裂体的选取无关，因此在讨论这问题时，我们就可以不考虑它所在的分裂体。

由 § 3.10 我们得知，$f(x)$ 有重零点的必要充分条件是 $f(x)$ 与 $f'(x)$ 有次数大于零的公因式，但既约多项式不能与较低次多项式有次数大于零的公因式。因此既约多项式 $f(x)$ 有重零点的必要充分条件是 $f'(x)=0$.

假设既约多项式 $f(x)=\sum_{i=0}^{n}a_ix^i$，如果 $f'(x)=\sum_{i=1}^{n}ia_ix^{i-1}=0$，那末

$$ia_i=0,\quad i=1,\ 2,\ \cdots,\ n.$$

当 F 的特征数是零时，我们有

$$a_i=0,\quad i=1,\ 2,\ \cdots,\ n.$$

于是 $f(x)=a_0$，因此 $f(x)$ 是 $F[x]$ 中可逆元，这与 $f(x)$ 是既约的假设不合，所以 $f'(x)\neq 0$，因此这时既约多项式 $f(x)$ 没有重零点。当 F 的特征数是 p 时，如果 $a_i\neq 0$，我们就有

$$i\equiv 0(p),$$

因此

$$f(x)=a_0+a_px^p+a_{2p}x^{2p}+\cdots,$$

也就是说，这时 $f(x)$ 是 x^p 的多项式。反过来，如果 $f(x)$ 是 x^p 的多项式，那末 $f'(x)=0$，因此它有重零点。于是我们有

定理 1　可换体 F 的特征数如果是零，那末 $F[x]$ 中既约多项式没有重零点；如果是 p，那末 $F[x]$ 中既约多项式有重零点的必要充分条件是：它是 x^p 的多项式.

于是在特征数是 p 的可换体中，既约多项式有的是有重零点的．我们再要问，有重零点的，它的零点是否都是重零点？

假设既约多项式 $f(x)$ 是 x^p 的多项式，我们把它写成 $f(x)=h(x^p)$．如果 $h(x)$ 又是 x^p 的多项式，那末 $f(x)$ 就是 x^{p^2} 的多项式．现在假定 $f(x)$ 是 x^{p^k} 的多项式而不是 $x^{p^{k+1}}$ 的多项式，我们用

$$f(x)=g(x^{p^k})$$

来表示．因为 $f(x)$ 是既约的，所以 $g(x)$ 也是既约的．再假如 $g'(x)=0$，那末 $g(x)$ 又是 x^p 的多项式，因此 $f(x)$ 就是 $x^{p^{k+1}}$ 的多项式了，这与假设不合．因此 $g'(x)\neq 0$，所以这时既约多项式 $g(x)$ 没有重零点.

假定 $g(y)$ 的次数是 n_0，首项系数是 1（F 的单位元），在它的分裂体中，它分裂为 1 次因式 $y-\beta_i$ 的乘积，即

$$g(y)=\prod_{i=1}^{n_0}(y-\beta_i),$$

因此

$$f(x)=\prod_{i=1}^{n_0}(x^{p^k}-\beta_i).$$

如果 α_i 是 $x^{p^k}-\beta_i$ 的零点，也就是说 $\alpha_i^{p^k}=\beta_i$，那末

$$x^{p^k}-\beta_i=x^{p^k}-\alpha_i^{p^k}=(x-\alpha_i)^{p^k}.$$

于是

$$f(x)=\prod_{i=1}^{n_0}(x-\alpha_i)^{p^k}.$$

所以 $f(x)$ 有 n_0 个互异的零点 $\alpha_1, \cdots, \alpha_{n_0}$，并且它们都是 p^k 重零点．因此我们有

定理 2　假定可换体 F 的特征数是 p，$F[x]$ 中既约多项式 $f(x)$ 有重零点，那末 $f(x)$ 的零点都是重零点，并且有相同的重数 p^k.

上面 $g(y)$ 的次数 n_0 是既约多项式 $f(x)$ 相异零点的个数，叫做 $f(x)$（或 α_i）的**缩减次数**．p^k 是 $f(x)$ 零点的**重数**，k 叫做 $f(x)$（或 α_i）关于 F 的**指数**．显然，$f(x)$ 的次数是 n．次数 n，缩减次数 n_0 及指数 k 之间有如下关系：

$$n=n_0p^k.$$

$F[x]$ 中既约多项式 $f(x)$ 如果没有重零点，就叫做 F 的**可离多项式**，否则就叫做 F 的**不可离多项式**．可离多项式的零点叫做**可离元**，不可离多项式的零点叫做**不可离元**．当 F 的特征数是零时，它的既约多项式都是可离的，因此 F 的代数元都是可离元．当 F 的特征数是 p 时，指数是零的既约多项式是可离的，既约多项式是不可离的必要充分条件是：它是 x^p 的多项式．

假如 α 是指数为 k 的 F 的不可离元，那末 α^{p^r}，$1\leqslant r\leqslant k-1$，仍然是 F 的不可离元，但 α^{p^k} 就是 F 的可离元．也就是说，不可离元 α 的指数 k 是使 α^{p^k} 成为可离元的最小正整数，这是因为，如果 $f(x)=g(x^{p^k})$ 是 $F[x]$ 中 α 适合的既约多项式，那末 α^{p^k} 满足 $g(x)=0$，即 $g(\alpha^{p^k})=0$，但 $g(x)$ 是可离多项式，所以 α^{p^k} 是可离元．再 α^{p^r} 满足 $g(x^{p^{k-r}})=0$，因为 $g(x^{p^k})$ 是既约的，所以 $g(x^{p^{k-r}})$ 也是既约的，又因为 $g(x^{p^{k-r}})$ 是 x^p 的多项式，所以它是不可离多项式，因此 α^{p^r} 就是不可离元．

再假如 F 是特征数 p 的可换体，$\alpha^{p^k}\in F$，但 $\alpha^{p^{k-1}}\in F$，那末多项式

$$x^{p^k}-\alpha^{p^k}=(x-\alpha)^{p^k}$$

在 $F[x]$ 中是既约的．这是因为，如果它是可约，$g(x)$ 是它的既约因式，因零点重数是 p 的幂，所以 $g(x)=x-\alpha$ 或 $g(x)=(x-\alpha)^{p^l}$，$l<k$，这与 $\alpha^{p^{k-1}}\in F$ 的假设不合，因此 $x^{p^k}-\alpha^{p^k}$ 是既约的．

上面是介绍可离多项式、不可离多项式的概念及它们的基本性质，现在我们引用它来讨论代数体的构造．

体 F 的可换代数体．如果其中任意元是 F 的可离元时，就叫做 F 的**可离体**，否则就叫做 F 的**不可离体**．特别，可换体 F，如果它的任意代数元都是可离元，也就是说，如果 $F[x]$ 中任意既约多项式都是 F 的可离式时，叫做**完全体**，否则叫做**不完全体**．显然，特征数是零的体是完全体．完全体的代数体是这完全体的可离体．在代数体中，可离体是重要的一类，并且常常引用的体很多都是属于这一类．

我们容易知道，由不可离元扩张的体显然是不可离体，但是由可离元扩张的体是否就是可离体？下面我们根据映射的个数(定理5)这个重要性质来解答这问题．

假设 α 是 $F[x]$ 中既约多项式 $f(x)$ 在 $L=F(\alpha)$ 中的零点．如果 $f(x)$ 的缩减次数是 n_0，那末 $f(x)$ 在它的分裂体 $K\supseteq L$ 中有互异的 n_0 个零点，因此 L 在 K 中有 n_0 个互异的同值映射，但是在 K 或 K 的扩张体中，L 的互异同值映射是否只有这 n_0 个？

定理 3 假设 α 是关于 F 缩减次数为 n_0 的元，那末适当选取 $F(\alpha)$ 的扩张体，在其中可使 $F(\alpha)$ 关于 F 的同值映射互异的能有 n_0 个．但不论 $F(\alpha)$ 的扩张体如何选取，在其中，$F(\alpha)$ 关于 F 的互异同值映射不能多于 n_0 个．

证明 假定 $f(x)$ 是 $F[x]$ 中 α 适合的既约多项式，如果 $F(\alpha)$ 的扩张体选取 $f(x)$ 的分裂体，显然在其中 $F(\alpha)$ 就有 n_0 个互异的同值映射．但在 $F(\alpha)$ 的任意扩张体中，$F(\alpha)$ 关于 F 的任意同值映射把 α 变为同一既约多项式 $f(x)$ 的零点 α_k，因此把 $F(\alpha)$ 中任意元 $\sum a_i\alpha^i$ 变为 $\sum a_i\alpha_k^i$，也就是说，把 $F(\alpha)$ 射到 $F(\alpha_k)$，这映射就是上面 n_0 个同值映射中把 α 变为 α_k 的同值映射，所以 $F(\alpha)$ 在它的任意扩张体中不能有多于 n_0 个关于 F 互异的同值映射，因此定理成立．

一般我们有

定理 4　假设 $K=F(\alpha_1, \cdots, \alpha_n)$，$\alpha_i$ 是关于 $F_{i-1}=F(\alpha_1, \cdots, \alpha_{i-1})$ 缩减次数为 m_i 的元，$i=1, \cdots, n$，那末适当选取 K 的扩张体，在其中 K 关于 F 的互异同值映射有 $\prod_{i=1}^{n} m_i$ 个．但不论 K 的扩张体如何选取，在其中 K 关于 F 的互异同值映射不能多于 $\prod_{i=1}^{n} m_i$ 个．

证明　我们用归纳法来证明．当 $n=1$ 时就是上面的定理 3，因此这时定理成立．现在假定 $n-1$ 时定理成立，也就是说，在 F_{n-1} 的适当扩张体中，F_{n-1} 关于 F 的互异同值映射有 $\prod_{i=1}^{n-1} m_i$ 个，但不论如何不能比这更多．因为 K 关于 F 的任一同值映射产生 F_{n-1} 关于 F 的一个同值映射，因此 K 关于 F 的任一同值映射可以看成为 F_{n-1} 关于 F 的同值映射的延长．现在命 $\overline{F}_{n-1}$ 是 F_{n-1} 在 K 的适当扩张体中一个同值象，$g(x)$ 是 $F_{n-1}[x]$ 中 α_n 适合的既约多项式，$\bar{g}(x)$ 是 $\overline{F}_{n-1}[x]$ 中与 $g(x)$ 对应的多项式，$\bar{\alpha}_n$ 是在 K 的适当扩张体中 $\bar{g}(x)$ 的任意零点．因为 $F_{n-1}\cong\overline{F}_{n-1}$，所以 $F_{n-1}(\alpha_n)\cong\overline{F}_{n-1}(\bar{\alpha}_n)$，也就是说 $K\cong\overline{F}_{n-1}(\bar{\alpha}_n)$，因此对于 F_n 的一个同值映射我们有 m_n 个如此的延长．但不论如何不能比这更多．于是在 K 的适当扩张体中，K 关于 F 的互异同值映射有 $\prod_{i=1}^{n-1} m_i\cdot m_n=\prod_{i=1}^{n} m_i$ 个，但不论如何不能比这更多，因此定理成立．

于是我们得知，假如 $K=F(\alpha_1, \cdots, \alpha_n)$ 是 F 的代数体，那末在 K 的任意扩张体中，K 关于 F 的互异同值映射不能多于 $(K:F)$ 个．当每个 α_i 是 $F_{i-1}=F(\alpha_1, \cdots, \alpha_{i-1})$ 的可离元时，K 关于 F 的互异同值映射才有 $(K:F)$ 个．

假定在 $F(\alpha)$ 的适当扩张体中，$F(\alpha)$ 关于 F 互异同值映射的个数等于体的次数 $(F(\alpha):F)$．显然 α 是 F 的可离元，因此，在 $F(\alpha)$ 的适当扩张体中，$F(\alpha)$ 有 $(F(\alpha):F)$ 个关于 F 的互异同值映

射的必要充分条件是：α 是 F 的可离元．一般来说我们有

定理 5 在 $K=F(\alpha_1, \cdots, \alpha_n)$ 的适当扩张体中，K 有 $(K:F)$ 个关于 F 的互异同值映射的必要充分条件是：α_i 是

$$F_{i-1}=F(\alpha_1, \cdots, \alpha_{i-1}), \quad i=1, 2, \cdots, n$$

的可离元．

证明 条件的充分性已经知道成立，下面我们只用归纳法来证明必要性．

我们知道，K 关于 F 的任意同值映射可以看成是 F_{n-1} 关于 F 的同值映射的延长．根据假设，在 K 的适当扩张体中，K 关于 F 的同值映射有 $(K:F)$ 个，因此 F_{n-1} 关于 F 的同值映射有 $(F_{n-1}:F)$ 个，并且 F_{n-1} 关于 F 的任意同值映射有 $(K:F_{n-1})$ 个延长成为 K 关于 F 的同值映射，因为不这样，K 关于 F 的同值映射就不能有 $(K:F)$ 个，这与假设不合．因此由归纳法假设，α_i 是 F_{i-1} 的可离元，所以条件的必要性成立，因此定理得证．

要注意的是，K 关于 F 互异的同值映射的个数是 K 的内在性质，它与 α_i 的选择无关．现在我们来讨论上面提出的问题．

定理 6 假设 $K=F(\alpha_1, \cdots, \alpha_n)$，$\alpha_i$ 是 $F_{i-1}=F(\alpha_1, \cdots, \alpha_{i-1})$，$i=1, 2, \cdots, n$ 的可离元，那末 K 是 F 的可离体．

证明 由定理 5 的充分条件，我们得知在适当扩张体中，K 关于 F 的互异同值映射有 $(K:F)$ 个．假定 $\beta(=\beta_1)$ 是 K 中任意元，我们可以适当地选取 β_i 使 $K=F(\beta_1, \beta_2, \cdots, \beta_m)$，根据定理 5 的必要条件，$\beta$ 是 F 的可离元，因此定理成立．

假如 α_i 是 F 的可离元，显然它也是 F_{i-1} 的可离元，因此如果 $\alpha_1, \cdots, \alpha_n$ 都是 F 的可离元，那末 $F(\alpha_1, \cdots, \alpha_n)$ 是 F 的可离体，这就是说，由可离元扩张的体是可离体．于是在 F 的可换代数体 K 中，F 的可离元的和，差，积，商仍然是 F 的可离元．

在 §4.5 中，我们知道代数体这个关系是适合传递律的，可离

体这关系也适合传递律，即

定理 7 假如 K 是 L 的可离体，L 是 F 的可离体，那末 K 是 F 的可离体.

证明 因为 K 中任意元 α 是 L 的可离元，假定 $\alpha_1, \cdots, \alpha_n$ 是 $L[x]$ 中 α 适合的既约多项式的系数，因为它们都是 F 的可离元，并且 α 是 $F(\alpha_1, \cdots, \alpha_n)$ 的可离元，由定理 6, $F(\alpha_1, \cdots, \alpha_n, \alpha)$ 是 F 的可离元，所以 α 是 F 的可离元，因此定理得证.

假如 K 是 F 的可换代数体，那末在 K 中，所有 F 的可离元形成一子体 L，显然，L 是 K、F 的中间体，并且它是 K 中 F 的**最大可离体**，$(L:F)$ 叫做 K 关于 F 的**缩减次数**. 我们容易得知，K 是 F 的可离体的必要充分条件是：K 关于 F 的次数 $(K:F)$ 等于 K 关于 F 的缩减次数 $(L:F)$，即 $(K:F)=(L:F)$. 再由定理 7，我们容易得知 K 中除 L 中元外，任意元都是 L 的不可离元，象 K 这样的 L 扩张体叫做 L 的**纯不可离体**，于是代数扩张可以由先可离扩张，然后再纯不可离扩张而成.

假如 F 的可换代数体 K 中元关于 F 的指数有最大值，那末这最大指数，我们又叫做 K 关于 F 的**指数**.

假定可换体 F 的特征数是 p, $K=F(\alpha)$，如果 α 关于 F 的指数是 k，那末 K 关于 F 的指数就是 k. 这是因为，K 中任意元可以写成 $\sum a_i\alpha^i$，由于 $a_i^{p^k}$ 及 α^{p^k} 都是 F 的可离元，所以

$$(\sum a_i\alpha^i)^{p^k}=\sum a_i^{p^k}(\alpha^{p^k})^i$$

也是 F 的可离元，于是 $\sum a_i\alpha^i$ 关于 F 的指数不大于 k. 因此 K 中元关于 F 的最大指数就是 k. 假如 K 中 F 的最大可离体是 L，那末 $(K:L)=p^k$，因此

$$(K:F)=(L:F)p^k.$$

这是因为 α^{p^k} 是 F 的可离元，而 $\alpha^{p^{k-1}}$ 是 F 的不可离元，即 $\alpha^{p^k}\in L$,

$\alpha^{p^{k-1}} \in L$，所以，$x^{p^k}-\alpha^{p^k}$ 在 $L[x]$ 中是既约的．一般，假如 $K=F(\alpha_1, \cdots, \alpha_n)$，$\alpha_i$ 关于 F 的指数是 k_i，显然 $k_1, \cdots, k_n$ 中最大数就是 K 关于 F 的指数．再假如 L 是 K 中 F 的最大可离体，那末 $(K:L)=p^f$，因此

$$(K:F)=(L:F)p^f, \quad f\geqslant k,$$

这里 k 是 K 关于 F 的指数．这是因为，$(L(\alpha_1):L)=p^{k_1}$，假如命 $L[x]$ 中既约多项式 $x^{p^{k_2}}-\alpha_2^{p^{k_2}}=(x-\alpha_2)^{p^{k_2}}$ 在 $L(\alpha_1)[x]$ 的既约因式是 $x^{p^{k_2'}}-\alpha_2^{p^{k_2'}}=(x-\alpha_2)^{p^{k_2'}}$，$k_2'\leqslant k_2$，那末 $(L(\alpha_1, \alpha_2):L(\alpha_1))=p^{k_2'}$，因此 $(L(\alpha_1, \alpha_2):L)=p^{k_1+k_2'}$，再这样继续进行，最后我们有 $(K:L)=p^f$，这里 $f=k_1+k_2'+\cdots+k_n'$，显然 $f\geqslant k$．

习 题 4.7

1．假定 F 是特征数 p 的体，x 是未定元．试证多项式 y^p-x 在 $F(x)[y]$ 中是既约的，并且 $F(x^{\frac{1}{p}})$ 是 $F(x)$ 的不可离体．

2．假如 α 关于 F 的指数是 k，那末 α^p 关于 F 的指数是 $k-1$．

3．假定 F 是特征数 p 的体，$f(x)=\sum a_i x^i$ 是 $F[x]$ 中的可离多项式．试证 $g(x)=\sum a_i^p x^i$ 也是 $F[x]$ 的可离多项式．因此可离元的任意 p 次幂仍然是可离元．

4．假如特征数 p 的体 K 中各元的 p 乘幂形成的体是 K^p，试证 K 是完全体的必要充分条件是 $K=K^p$．

5．试证任意完全体的代数体是完全体，任意不完全体的有穷次体是不完全体．

6．假如 K 是 F 的纯不可离体，试证 K 是 F 的正规体，并且在任一扩张体中，K 关于 F 的同构映射是恒等映射．

7．假如 F 是特征数 p 的体，α 是纯多项式 $x^{p^k}-a$，$a\in F$ 的零点，试证 $F(\alpha)$ 是 F 的纯不可离体．

8．假定 K 是 F 的代数体．$K\supseteq L\supseteq F$，K 关于 L 的缩减次数是 m，L 关于 F 的缩减次数是 n，试证 K 关于 F 的缩减次数是 mn．

§ 4.8 有穷次扩张体的单纯性

我们知道在扩张体中，单扩张是构造最简单的．有的扩张体形状上虽然不是单扩张，但我们可以把它改写成单扩张，这样在讨论时很多问题就能够简化．因此我们要问，怎样的扩张体能够改写成单扩张？

我们容易得知，于 F 添加两个超越元扩张的体不是 F 的单扩张，添加一个代数元及一个超越元扩张的体也不是 F 的单扩张．此外，F 的无穷次代数体显然也不是 F 的单扩张，因此单扩张也就是本原元，只有在有穷次代数体中来讨论了．

假定 K 是 F 的有穷次代数体．如果 F 只含有穷个元，那末 K 也只含有穷个元．在下节中我们就知道，元数是有穷的体是有本原元的，因此在这节我们假定 F 含无穷个元．

下面是本原元的一个充分条件．

定理 1 假如 $K=F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 是 F 的有穷次可换代数体，$\alpha_2, \cdots, \alpha_n$ 是 F 的可离元，那末 K 有关于 F 的本原元．

证明 我们用数学归纳法来证明．当 $n=1$ 时，定理显然成立．

当 $n=2$ 时，为了方便，我们把 α_1, α_2 分别写成 α, β．假定 $f(x), g(x)$ 是 $F[x]$ 中零点分别为 α, β 的既约多项式，并且在包含 $f(x), g(x)$ 的分裂体的扩张体中．我们假定 $f(x)$ 的零点是 $\alpha_1=\alpha, \alpha_2, \cdots, \alpha_r$，$g(x)$ 的零点是 $\beta_1=\beta, \beta_2, \cdots, \beta_s$．因为 $\beta\neq\beta_i$，$i\neq1$，所以对于任意 i 及 $j(\neq1)$，多项式

$$\alpha_i+x\beta_j=\alpha+x\beta$$

在 F 中最多只有一个零点．但 F 中含无穷个元，因此 F 中有不适合这式的元．假如 a 是这样的一元，即

$$\alpha_i+a\beta_j\neq\alpha+a\beta,\quad j\neq 1.$$

命 $\gamma=\alpha+a\beta$, 于是

$$F(\gamma)\subseteq F(\alpha,\ \beta).$$

如果我们能够证明 $\beta\in F(\gamma)$, 那末 $\alpha=\gamma-a\beta\in F(\gamma)$, 因此 $F(\alpha,\ \beta)=F(\gamma)$, 于是 γ 就是所求的本原元了.

因为 $\qquad g(\beta)=0,\quad f(\alpha)=f(\gamma-a\beta)=0,$

所以 β 是 $F(\gamma)[x]$ 中多项式 $g(x)$, $f(\gamma-ax)$ 的公共零点. 但当 $j\neq 1$ 时, $\gamma-a\beta_j\neq\alpha_i$, 因此

$$f(\gamma-a\beta_j)\neq 0.$$

于是 $g(x)$, $f(\gamma-ax)$ 在 $F(\gamma)$ 中只有一个公共零点 β, 所以 $g(x)$, $f(\gamma-ax)$ 只有一个 1 次公因式 $x-\beta$, 也就是说, $x-\beta$ 是 $g(x)$, $f(\gamma-ax)$ 的最大公因式. 再因为 $g(x)$, $f(\gamma-ax)$ 的系数都在 $F(\gamma)$ 中, 因此它们的最大公因式的系数也都在 $F(\gamma)$ 中, 于是 $\beta\in F(\gamma)$, 所以 $n=2$ 时定理成立.

假如在 $n-1$ 时定理成立, 命 $F(\alpha_1,\ \cdots,\ \alpha_{n-1})=F(\alpha)$, 那末

$$F(\alpha_1,\ \cdots,\ \alpha_{n-1},\ \alpha_n)=F(\alpha,\ \alpha_n)=F(\gamma),$$

这就是说在 n 时定理成立, 因此定理得证.

譬如 $Q(\sqrt{2},\ \sqrt{3})=Q(\sqrt{2}+\sqrt{3})$, 其中 Q 是有理数体, 这性质我们也可这样来验证, 因为 $\gamma=\sqrt{2}+\sqrt{3}$, $\gamma^3=11\sqrt{2}+9\sqrt{3}$, 所以 $\sqrt{2}$, $\sqrt{3}$ 都能够用 γ 的多项式表出.

于是我们得知有穷次可离体是单扩张体, 特征数是零的体的有穷次体也是单扩张体. 对于特征数是 p 的有穷次体, 我们有

定理 2 假定体 F 的特征数是 p, K 是 F 的 n 次可换代数体, 那末 K 是 F 的单扩张体的必要充分条件是

$$n=n_0p^k,$$

这里 n_0 及 k 分别是 K 关于 F 的缩减次数及指数.

证明 假定 K 是 F 的单扩张体, $K=F(\alpha)$, k 是 α 关于 F 的

指数，也就是 K 关于 F 的指数，L 是 K 中 F 的最大可离体，由 § 4.7 我们有 $(K:F)=(L:F)p^k$，因此 $n=n_0p^k$，所以条件的必要性成立．

反过来，假定 $n=n_0p^k$，因为 L 是 F 的有穷次可离体，所以它是 F 的单扩张体，我们命 $L=F(\alpha)$．再假定 β 是 K 中关于 F 指数为 k 的元，那末 $(L(\beta):L)=p^k$，因此 $(L(\beta):F)=n_0p^k$，于是 $K=L(\beta)$，所以 $K=F(\alpha, \beta)$．但 α 是 F 的可离元，由定理 1，K 有关于 F 的本原元，这就是说 K 是 F 的单扩张体，所以条件的充分性成立，因此定理得证．

下面是关于单扩张中间体的一个重要性质．

定理 3 假定 $F(\alpha)$ 是 F 的代数体，K 是 $F(\alpha)$，F 的中间体，那末 K 是 F 的单扩张体．

证明 当 F 的特征数是零时，定理显然成立，下面我们引用定理 2 就 F 的特征数是 p 的情况来证明．

假定 k, k' 分别是 α 关于 F, K 的指数，k'' 是 K 关于 F 的指数．因为 $F(\alpha)$ 关于 F, K 都是单扩张，由定理 2，我们得知 $F(\alpha)$ 关于 F, K 的缩减次数分别是 $(F(\alpha):F)p^{-k}$, $(F(\alpha):K)p^{-k'}$．于是由 § 4.7，习题 8，K 关于 F 的缩减次数是 $(K:F)p^{-(k-k')}$，因此 $k-k'\geqslant k''$．

如果我们能够证明 $k-k'\leqslant k''$，也就是 $k'+k''\geqslant k$，那末 $k-k'=k''$，于是由定理 2，K 就是 F 的单扩张体，因此定理就告成立．

因为 $\alpha^{p^{k'}}$ 是 K 的可离元，我们命 $f(x)$ 是 $K[x]$ 中 $\alpha^{p^{k'}}$ 适合的可离多项式，因为 $(f(x))^{p^{k''}}=g(x^{p^{k''}})$，$f(\alpha^{p^{k'}})=0$，所以 $g(\alpha^{p^{k'+k''}})=0$，再因为 $f(x)$ 是可离多项式，由 § 4.7 习题 3，得知 $g(x)$ 也是可离的，因此 $\alpha^{p^{k'+k''}}$ 是 F 的可离元，但 α 关于 F 的指数是 k，所以 $k'+k''\geqslant k$．于是定理成立．

习 题 4.8

1. 试求 $Q(\sqrt{3}, \sqrt[3]{2})$ 的本原元，这里 Q 是有理数体。

2. 试求 $Q(i, \sqrt{2})$ 的本原元.

3. 假如 x, y 是未定元，试证 $F(x, y)$ 的扩张体 $F(x^{\frac{1}{p}}, y^{\frac{1}{p}})$ 没有本原元，这里 p 是 F 的特征数。

§4.9 有 穷 体

我们知道元数是有穷的体叫做有穷体，有时我们又叫做伽罗瓦域，这节我们讨论有穷体的构造.

假设 K 是有穷体，显然它包含的质体 F 也是有穷体，因为特征数是零的质体与有理数体同构，它不是有穷体. 因此 K 的特征数异于零. 我们假定 K 的特征数是 p.

再因为 K 只含有穷个元，显然其中关于 F 线性无关的元也只能是有穷个，因此 K 关于 F 是有穷次的. 假如 $(K:F)=n$, $\alpha_1, \cdots, \alpha_n$ 是 K 关于 F 的底，那末 K 中任意元能够一意地表成下面形状:

$$a_1\alpha_1+\cdots+a_n\alpha_n, \quad a_i\in F.$$

因为 a_i 只能取 p 个值，所以象上面形状的元互异的只有 p^n 个，因此 K 的元数 $q=p^n$.

于是我们得到

定理 1 假如 K 是元数为 q 的有穷体，它的质体是 F，那末它的特征数 $p\neq 0$，并且 $q=p^n$，这里 $n=(K:F)$.

我们知道元数是有穷的群以及元数是有穷的环都不一定是可换的. 譬如对称群 S_n 就不是可换群. 假如 $R=Z-(p)$，p 是质数，那末全矩阵环 R_n 也不是可换环，但是元数是有穷的体却不是

这样．任意有穷体都是可换体，这结论是 1905 年魏特邦 (J. H. M. Wedderburn, 1882～1948) 提出的，是魏特邦著名定理之一．因为证明比较麻烦，我们把证明放在这节后面，在这里我们先承认这个事实好了．

假定有穷体 K 的元数是 q，那末它的乘群的元数就是 $q-1$，于是 K 中任意非零元 α 的阶数是 $q-1$ 的因数，因此

$$\alpha^{q-1}=e,\quad \alpha\neq 0,$$

所以

$$\alpha^q=\alpha.$$

显然 $\alpha=0$ 也是这多项式的零点，这就是说，在元数是 q 的有穷体中，任意元的 q 次幂仍然是它自身．于是 K 中元都是 $F[x]$ 中多项式 x^q-x 的零点，因此 K 是多项式 x^q-x 的分裂体．根据 § 4.6 定理 3，我们又有

定理 2　元数相等的有穷体是同构的．

我们知道有穷体的元数是质数的乘幂，反过来，假如 p 是任意质数，用它的任意正整数幂 p^n 做元数的有穷体是否存在？

由 § 4.2，元数是 p 的质体 F 是存在的．从 F 作 $F[x]$ 中多项式 $f(x)=x^{p^n}-x$ 的分裂体 K，假如 α, β 是 $f(x)$ 在 K 的零点，即 $\alpha^{p^n}=\alpha$, $\beta^{p^n}=\beta$，那末

$$(\alpha-\beta)^{p^n}=\alpha^{p^n}-\beta^{p^n}=\alpha-\beta,$$

并且当 $\beta\neq 0$ 时，

$$\left(\frac{\alpha}{\beta}\right)^{p^n}=\frac{\alpha^{p^n}}{\beta^{p^n}}=\frac{\alpha}{\beta}.$$

这就是说，在 K 中，$f(x)$ 的任意两个零点的差及商仍然是它的零点，因此 K 中 $f(x)$ 的所有零点形成体．再因为

$$f'(x)=p^nx^{p^n-1}-e=-e,$$

因此 $f(x)$ 没有重零点，也就是说，$f(x)$ 的 p^n 个零点是互异的．所以 K 是元数为 p^n 的体，于是我们有

定理 3 对于任意质数 p 的乘幂 p^n，除同构的外，只有唯一个元数是 p^n 的有穷体，也就是伽罗瓦域.

因为一个伽罗瓦域由它的元数唯一决定，元数是 p^n 这类型的伽罗瓦域我们用 $GF(p^n)$ 来表示，下面我们来讨论它的子体.

假如 K 是 $GF(p^n)$ 的子体，那末 K 也是伽罗瓦域. 因为 K 的特征数与 $GF(p^n)$ 的特征数相同，所以 K 的特征数也是 p，因此 K 是伽罗瓦域 $GF(p^m)$. 这时因为 $m=(K:F)$，所以 m 是 n 的因数，这就是说，$GF(p^n)$ 的子体只有象 $GF(p^m)$ 这样的，其中 m 是 n 的因数. 现在我们要问，对于 n 的任意因数 m，$GF(p^m)$ 是否是 $GF(p^n)$ 的子体？下面的解答与 §2.2 定理 5 中有穷群的情况类似.

定理 4 假设 m 是 n 的任意因数，那末 $GF(p^n)$ 中只有唯一个 $GF(p^m)$ 型子体.

证明 因为 m 是 n 的因数，所以

$$p^n-1=(p^m-1)(p^{n-m}+p^{n-2m}+\cdots+p^m+1),$$

于是 $x^{p^m-1}-1$ 是 $x^{p^n-1}-1$ 的因数，因此 $x^{p^m}-x$ 是 $x^{p^n}-x$ 的因式，但 $x^{p^n}-x$ 在 $GF(p^n)$ 中完全分裂，所以 $x^{p^m}-x$ 在 $GF(p^n)$ 中也完全分裂，于是 $GF(p^n)$ 中包含 $x^{p^m}-x$ 的 p^m 个零点，由这 p^m 个零点形成的子体就是伽罗瓦域 $GF(p^m)$. 再因为 $x^{p^m}-x$ 在 $GF(p^n)$ 中的分裂体只有唯一个，因此 $GF(p^n)$ 中只有唯一个 $GF(p^m)$ 型子体，所以定理得证.

于是我们得知伽罗瓦域 $GF(p^n)$ 中子体的个数等于 n 中互异正因数的个数. 在群中，循环群的构造以及它的子群的个数是已经知道了的，与这类似，在体中，对于伽罗瓦域，这两个问题也算是解决了的.

后面我们需要下列一些性质，但这些性质本身也有广泛应用.

定义　假设 e 是可换体 F 的单位元，h 是正整数，那末

$$f(x)=x^h-e$$

在 F 的扩张体中的零点，叫做 F 的 h 次单位根，有时简单地叫做 h 次单位根.

当 h 与 F 的特征数互质(F 的特征数是零时，h 可以是任意正整数)时，因为 $f'(x)=hx^{h-1}$，显然 $f(x)$ 没有重零点，因此在 $f(x)$ 的分裂体中，h 次单位根恰有 h 个.

在 §2.2 中，我们得知复数体中 n 次单位根形成 n 元循环群，这性质在一般可换体中也成立.

定理 5　假定 h 是与 F 的特征数互质的正整数，那末在 F 的适当扩张体中，F 的所有 h 次单位根形成元数是 h 的循环群.

证明　假设 $\alpha^h=e$，$\beta^h=e$，那末

$$(\alpha\beta^{-1})^h=\alpha^h\beta^{-h}=e,$$

因此 x^h-e 的所有零点对乘法形成一个元数是 h 的群 G. 我们把 h 分解为质数 p_i 的乘积，即 $h=\prod_{i=1}^{m}p_i^{r_i}$. 假如在 G 中我们能够找到阶数是 $p_i^{r_i}$ 的元 a_i，由 §2.2 习题 5，$a=\prod_{i=1}^{m}a_i$ 就是 G 中阶数是 h 的元，因此 $G=(a)$，于是 G 就是循环群了.

由 §3.10，我们知道 n 次多项式在可换体中零点不能多于 n 个，因此多项式

$$x^{\frac{h}{p_i}}-e$$

在 G 中最多只有 $\frac{h}{p_i}$ 个零点，于是 G 中最少有一个使 $b_i^{\frac{h}{p_i}}\neq e$ 的元 b_i，我们把 $b_i^{\frac{h}{p_i^{r_i}}}$ 写成 a_i，即 $a_i=b_i^{\frac{h}{p_i^{r_i}}}$. 因为 $a_i^{p_i^{r_i}}=b_i^h=e$，所以由 §2.2 习题 3，a_i 的阶数是 $p_i^{r_i}$ 的因数，但

$$a_i^{p_i^{r_i-1}}=b_i^{\frac{h}{p_i}}\neq e,$$

因此 $a_i^{p_i^{s_i}}\neq e$, $s_i<r_i$. 于是 a_i 的阶数是 $p_i^{r_i}$,所以定理得证.

由上面的证明，我们容易得知 G 所以能够成为循环群是因为其中满足 $x^{\frac{h}{p_i}}=e$ 的元不多于 $\frac{h}{p_i}$ 个. 反过来，假如 $G=(a)$ 是 n 元循环群，m 是 n 的任意因数，显然其中满足 $x^m=e$ 的元只有 $a^{\frac{n}{m}i}$, $i=0, 1, \cdots, m-1$. 因此 n 元可换群 G 是循环群的必要充分条件是：对于 n 的任意因数 m, G 中满足 $x^m=e$ 的元不多于 m 个. 在 § 2.2 中我们给出了循环群的一个必要充分条件. 这里我们又得到另一个必要充分条件.

阶数是 h 的 h 次单位根，叫做 **h 次本原单位根**. 我们知道，假如 α 是 K 中 h 次本原单位根，那末 α^m 是 h 次本原单位根的必要充分条件是 m 与 h 互质，即 $(m, h)=1$. 因此，在 K 中 h 次本原单位根的个数等于 $\varphi(h)$.

要注意的是，假如 F 的特征数是 p, $h=qp^k$, $(q, p)=1$. 因为 $x^h-1=(x^q-1)^{p^k}$, 所以这时 F 没有阶数是 h 的单位根，也就是说没有 h 次本原单位根. 因此如果 F 含有 h 次本原单位根，那末 h 与 p 就互质.

现在我们引用上面的结论，推得下面伽罗瓦域的一些性质.

因为 $GF(p^n)$ 的乘群 G 中元都是多项式 $x^{p^n-1}-e$ 的零点，由定理 5, 我们得知 G 是循环群，这就是说有穷体的乘群是循环群. 这是有穷体的一个重要性质. 由上面循环群的充分条件，我们又可以把这性质推广到任意可换体，也就是说，任意可换体的乘群的有穷子群都是循环群. 对于一般体，这性质不一定成立，譬如四元数体的有穷子群 $\{\pm e, \pm i, \pm j, \pm k\}$ 就不是循环群，但是也有乘群的任意可换有穷子群都是循环群的非可换体[12].

假定伽罗瓦域 $GF(p^n)$ 的乘群 $G=(\alpha)$, 那末 $GF(p^n)=F(\alpha)$,

因此 $GF(p^n)$ 关于质体 F 有本原元. 又因为 $x^{p^n}-x$ 没有重零点, 所以 α 是 F 的可离元, 于是 $GF(p^n)$ 是质体 F 的可离体. 但 $GF(p^n)$ 的任意子体 K 都包含 F, 所以 $GF(p^n)$ 又是 K 的可离体, 因此它又有关于 K 的本原元.

最后我们来证明魏特邦定理.

定理 6　有穷体是可换体.

这定理是 1905 年魏特邦首先证明的, 自后再来证明的颇不乏人, 下面所叙述的是 1931 年威特(E. Witt)提出的一个初等证明[13].

我们先介绍分圆多项式的一些性质, 以备引用.

假定 $\xi_1, \cdots, \xi_{\varphi(h)}$ 是 h 次复数本原单位根, 那末

$$\phi_h(x)=\prod_{i=1}^{\varphi(h)}(x-\xi_i)$$

叫做 **h 次分圆多项式**. 由计算容易得知,

$$\phi_1(x)=x-1,\qquad \phi_2(x)=x+1,$$
$$\phi_3(x)=x^2+x+1,\quad \phi_4(x)=x^2+1.$$

再我们有

$$x^h-1=\prod_{d\mid h}\phi_d(x),$$

式中 d 取 h 的所有正因数, 这是因为任意 h 次单位根是某个 d 次本原单位根. 反过来, 任意 d 次本原单位根都是 h 次单位根. 又分圆多项式 $\phi_h(x)$ 的系数都是整数, 这是因为, $\phi_1(x)=x-1$ 的系数是整数, 如果对于 $0<d<h$, $\phi_d(x)$ 的系数是整数, 由 §3.5, 我们得知用首项系数是 1 的整系数多项式 $\prod\limits_{d\neq h}\phi_d(x)$ 除整系数多项式 x^h-1 得到的商 $\phi_h(x)$ 仍然是整系数多项式.

又假定 q 是不小于 2 的有理数. 如果 $h=1$, 那末

$$|\phi_h(q)|=q-1;$$

如果 $h>1$, 我们命 ξ 是 h 次本原单位根, 即

$$\xi=\cos\frac{2k\pi}{h}+i\sin\frac{2k\pi}{h},\quad (k,\ h)=1,$$

因为

$$|q-\xi|^2=\left(q-\cos\frac{2k\pi}{h}\right)^2+\sin^2\frac{2k\pi}{h}$$
$$=q^2-2q\cos\frac{2k\pi}{h}+1>(q-1)^2,$$

所以
$$|q-\alpha|>q-1\geqslant 1,$$

因此，当 $h>1$ 时，$\quad |\phi_h(q)|=\prod_{i=1}^{\varphi(h)}|q-\xi_i|>q-1.$

现在来证明我们的定理.

假设 K 是有穷体，F 是它的中心，$(K:F)=n$，α 是 K 中任意非零的元，显然，K 中所有与 α 能够交换的元，即所有适合

$$x\alpha=\alpha x,\quad x\in K$$

的元 x 形成一个体 L，并且 $K\supseteqq L\supseteqq F$. 我们容易知道，如果 $\alpha\in F$，那末 $L=K$；反过来，如果 $L=K$，那末 $\alpha\in F$. 这就是说，$\alpha\in F$ 的必要充分条件是 $L=K$. 假定 F 的元数是 q，那末 K 及 L 的元数分别是 q^n，q^d，这里 $d=(L:F)$. 于是 $d|n$. 如果我们能够证明 $d=n$，那末 $L=K$，因此 $\alpha\in F$，于是 K 就是可换体了.

我们用反证法来证明. 假定 $d<n$，那末 $n>1$，我们把 K 的乘群分为若干个共轭类. 我们知道，如果 $\alpha\in F$，那末 α 自身成为一共轭类，如果 $\alpha\in F$，由 §2.4 得知 α 所在的共轭类的元数是 $\dfrac{q^n-1}{q^d-1}$，这里 $d\neq n$，于是

$$q^n-1=q-1+\sum_{d|n}\frac{q^n-1}{q^d-1},\quad d\neq n.$$

因为 $\phi_n(q)$ 是 q^n-1 的因数，并且当 $d<n$ 时，它不是 q^d-1 的因数，所以 q^n-1 及 $\dfrac{q^n-1}{q^d-1}$，$d<n$，都能够用 $\phi_n(x)$ 整除，因此 $q-1$

也能够用 $\phi_n(q)$ 整除，这与 $q\geqslant 2$, $n>1$ 时，$|\phi_n(q)|>q-1$ 的性质不合，因此 $n=d$，所以定理得证.

1945 年贾柯勃逊(N. Jacobson, 1910～)有这样一个定理：假定对于环 R 中任意元 a，我们有与 a 有关的整数 $n(a)>1$ 存在，使 $a^{n(a)}=a$，那末 R 就是可换环[14]．这定理可以说是上面魏特邦定理的推广．1954 年赫尔司顿(I. N. Herstain, 1923～)有一个初等证明．1971 年温沙(J. W. Wansley)另有一个初等证明[15]．上面的贾柯勃逊定理是环为可换环的一个充分条件而不是必要条件，1957 年赫尔司顿又给出了一个必要充分条件，1959 年富永久雄(1927～)对这有所推广．1971 年贝尔(H. E. Bell)又有推广[16]．读者如欲知其详，请取原始资料参考.

习 题 4.9

1．试证费马(P. D. Fermat, 1601～1665)定理：

$$a^{p-1}\equiv 1(p),$$

这里 p 是质数，a 是非零的整数.

2．假如 F 是特征数为 p 的质体，α 是 $F[x]$ 中 m 次既约多项式 $f(x)$ 在 $GF(p^n)$ 中的零点，试证 α^p, α^{p^2}, $\cdots$, $\alpha^{p^m}=\alpha$ 都是 $f(x)$ 的零点.

3．试证伽罗瓦域是完全体.

4．假如 K 是特征数为 p 的伽罗瓦域，a 是其中任意元，试证在 K 中，a 的 p 次根只有一个 $a^{\frac{1}{p}}$.

5．试证分圆多项式 $\phi_n(x)$ 是正规式.

6．试求作 $GF(3^2)$ 的加法及乘法表.

§4.10 超越扩张体

我们知道体 F 的扩张体如果不是 F 的代数扩张体，就叫做 F 的超越扩张体，前面五节讨论的主要是代数扩张体，这节我们来讨

论超越扩张体. 使用的方法及所得的结果都与§4.5的类似. 在讨论代数扩张体时，体的次数及底是两个基本概念，现在我们需要与它们类似的概念，因此首先我们把线性相关、线性无关的概念来推广.

假定u是F的扩张体K中元，M是K的有穷子集，如果u是体$F(M)$的代数元，那末u叫做关于F与M**代数相关**，否则就叫做关于F与M**代数无关**. 假如M中有一元关于F与其余元代数相关，那末M叫做关于F**代数相关**，否则就叫做关于F**代数无关**.

于是，假如α是F的代数元，那末它关于F代数相关；假如α是F的超越元，那末α关于F代数无关. 根据定义，我们容易得知，u关于F与$M=\{u_1, \cdots, u_m\}$代数相关的必要充分条件是：u是多项式

$$\sum_{i=0}^{n} f_i(u_1, \cdots, u_m)x^i, \quad f_n(u_1, \cdots, u_m) \neq 0$$

的零点，这里$f_i(x_1, \cdots, x_m)$是$F[x_1, \cdots, x_m]$中元.

显然，假如M关于F代数无关，那末它的任意子集关于F代数无关；假如M关于F代数相关，那末任意包含M的有穷集关于F代数相关. 再假如v关于F与M线性相关，那末u关于F与M代数相关；假如M关于F代数无关，那末M关于F线性无关.

下面是代数相关的基本性质，这些性质也是线性相关具备的.

1. 假定$v \in M$，那末u关于F与M代数相关.

这是因为v在$F(M)$中，所以u是关于$F(M)$的代数元，因此v关于F与M代数相关.

2. 假定v关于F与$M=\{u_1, \cdots, u_m\}$代数相关，但与$\{u_1, \cdots, u_{m-1}\}$代数无关，那末u_m关于F与$\{u_1, \cdots, u_{m-1}, v\}$代数相关.

这是因为 v 关于 F 与 M 代数相关，所以我们有

$$\sum_{i=0}^{r} f_i(u_1, \cdots, u_m) v^i = 0, \quad f_r(u_1, \cdots, u_m) \neq 0.$$

我们把上式左边多项式写成 u_m 的多项式 $\sum_{i=0}^{s} g_i(u_1, \cdots, u_{m-1}, v) u_m^i$，就得到

$$\sum_{i=0}^{s} g_i(u_1, \cdots, u_{m-1}, v) u_m^i = 0.$$

因为 v 关于 F 与 $\{u_1, \cdots, u_{m-1}\}$ 代数无关，所以所有的 $g_i(u_1, \cdots, u_{m-1}, v) \neq 0$，或所有的 $g_i(u_1, \cdots, u_{m-1}, x) = 0$，即 $g_i(u_1, \cdots, u_{m-1}, x)$ 的系数都为零．如果所有的 $g_i(u_1, \cdots, u_{m-1}, x) = 0$，那末

$$\sum_{i=1}^{r} f_i(u_1, \cdots, u_m) x^i = 0,$$

因此 $f_r(u_1, \cdots, u_m) = 0$，这与假设不合．于是所有的 $g_i(u_1, \cdots, u_{m-1}, v)$ 不能完全都是零，所以 u_m 关于 F 与 $\{u_1, \cdots, u_{m-1}, v\}$ 代数相关．

特别，假如关于 F，α 是超越元，并且与 β 代数相关，那末 β 关于 F 与 α 代数相关．

3．假定关于 F，v 与 M 代数相关，并且 M 中任意元与 N 代数相关，那末 v 关于 F 与 N 代数相关．

这是因为 v 是 $F(M)$ 的代数元时，它当然也是 $F(M, N)$ 的代数元．因此 $F(M, N)(v)$ 是 $F(M, N)$ 的代数体．但 $F(M, N)$ 是 $F(N)$ 的代数体，由 §4.5 定理 2，$F(M, N)(v)$ 是 $F(N)$ 的代数体，所以 v 是 $F(N)$ 的代数元，因此 v 关于 F 与 N 代数相关．

4．假定关于 F，M 代数无关，但 $M \cup u$ 代数相关，那末 u 与 M 代数相关．

这是因为关于 F，$M \cup u$ 代数相关，所以 $M \cup u$ 中某元 v 与 $M \cup u - v$ 代数相关．如果 $u = v$，那末 u 与 M 代数相关；如果 $u \neq v$，那末 $v \in M$，因为 M 代数无关，所以 v 与 $M - v$ 代数无关，因此

由 2, u 与 M 代数相关.

5. 假定关于 F, m 元集 M 代数无关, 并且 M 中任意元与有穷集 N 代数相关, 那末 N 的元数不小于 m.

这是因为关于 F, $M\cup N$ 中显然有代数无关的 m 元子集, 因为 M 就是这样的子集. 在所有这些 m 元子集中, 假设 M' 是含 N 中元最多的一个子集, 并且假定这最大元数是 $n(\geqslant 0)$. 假如 $n<m$, 我们命 u 是 M' 中而不是 N 中元, v 是 N 中任意元, 如果 $v\in M'-u$, 那末 v 与 $M'-u$ 代数相关; 如果 $v\bar{\in} M'-u$, 因为 m 元子集 $(M'-u)\cup v$ 含 N 中 $n+1$ 个元, 根据 n 是最大的假设, 我们得知 $(M'-u)\cup v$ 代数相关, 但 $M'-u$ 代数无关, 由 4 得知 v 与 $M'-u$ 代数相关, 这就是说 N 中任意元与 $M'-u$ 代数相关. 因为 $u\in M$, 根据假设 u 与 N 代数相关, 于是由 3, u 与 $M'-u$ 代数相关, 这与 M' 代数无关的假设不合, 因此 $n\geqslant m$. 即 N 的元数不小于 m.

上面的 M 都假定是有穷集, 假如 M 是无穷集, 如果 u 关于 F 与 M 的任意有穷子集代数无关, 那末 u 就叫做关于 F **与** M **代数无关**; 否则, 也就是说, u 关于 F 与 M 的某有穷子集代数相关, 那末 u 就叫做关于 F **与** M **代数相关**. 再如果 M 中任意有穷个元关于 F 都是代数无关, 那末 M 就叫做关于 F **代数无关**; 否则, 也就是说, M 中某有穷个元关于 F 代数相关, 那末 M 就叫做关于 F **代数相关**. 这与向量空间中无穷个元线性无关, 线性相关的概念完全一致.

下面是代数无关的一个基本性质.

我们知道, 一个元关于 F 代数无关的必要充分条件是它不适合 $F[x]$ 中任意非零的多项式. 一般这性质也是成立的.

定理 1 m 元集合 $M=\{u_1, \cdots, u_m\}$ 关于 F 代数无关的必要充分条件是对于 $F[x_1, \cdots, x_m]$ 中任意元 $f(x_1, \cdots, x_m)$, 如果 $f(u_1,$

$\cdots, u_m)=0$, 那末

$$f(x_1, \cdots, x_m)=0,$$

即 $f(x_1, \cdots, x_m)$ 的系数都是零.

证明　假如当 $f(u_1, \cdots, u_m)=0$ 时, $f(x_1, \cdots, x_m)=0$. 显然 M 中没有一元关于 F 与其余元代数相关, 所以 M 关于 F 代数无关, 因此条件的充分性成立.

再假如 M 关于 F 代数无关, 并且 $f(u_1, \cdots, u_m)=0$, 命

$$f(x_1, \cdots, x_m)=\sum_{i=1}^{n} f_i(x_1, \cdots, x_{m-1})x_m^i,$$

我们用归纳法来证明 $f(x_1, \cdots, x_m)=0$. 当 $m=1$ 时, f_i 是 F 中元, 因为 u_1 关于 F 代数无关. 所以 $f_i=0$. 因此 $f(x_1)=0$, 所以 $m=1$ 时条件的必要性成立. 假定 $m-1$ 时条件的必要性成立, 因为 M 关于 F 代数无关, 所以 $f_i(u_1, \cdots, u_{m-1})=0$, $i=1, 2, \cdots, n$. 又因为 $u_1, \cdots, u_{m-1}$ 关于 F 代数无关, 根据归纳法的假设, 我们有 $f_i(x_1, \cdots, x_{m-1})=0$, 于是 $f(x_1, \cdots, x_m)=0$, 因此条件的必要性成立. 所以定理得证.

于是 m 个元 $u_1, \cdots, u_m$, 如果是代数相关, 那末它们之间有代数方程相联系; 如果无关, 那末它们之间不存在任何代数方程的联系.

假定 $\{u_1, \cdots, u_n\}$ 关于 F 代数无关, $x_1, \cdots, x_n$ 是 F 的未定元, 显然

$$f(x_1, \cdots, x_n)\to f(u_1, \cdots, u_n)$$

是多项式环 $F[x_1, \cdots, x_n]$, $F[u_1, \cdots, u_n]$ 的同构. 于是它们的商体 $F(x_1, \cdots, x_n)$, $F(u_1, \cdots, u_n)$ 也同构, 也就是说 $F(x_1, \cdots, x_n)\cong F(u_1, \cdots, u_n)$. 因此代数无关的元我们可以看成未定元, 它们之间可以不加区别.

上面我们介绍了代数相关、代数无关的基本性质, 现在我们来

讨论超越扩张体.

定义 假定 K 是体 F 的扩张体，那末 K 中关于 F 代数无关子集的最大元数，叫做 K 关于 F 的**超越次数**. 假定 $M=\{u_1, \cdots, u_m\}$是 K 中关于 F 代数无关的子集，如果 K 中任意元关于 F 与 M 代数相关，那末 $u_1, \cdots, u_m$ 叫做 K 关于 F 的**代数底**.

因为 F 的代数体中任意元关于 F 代数相关，所以 F 的代数体关于 F 的超越次数是零，因此它没有关于 F 的代数底. 再假定 F 的超越单扩张体 $F(x)$ 中任意元 $u=\dfrac{f(x)}{g(x)}$，因为 $ug(x)-f(x)=0$，所以 u 与 x 关于 F 代数相关，于是由 5，用反证法得知 $F(x)$ 中任意两元关于 F 代数相关. 但 x 关于 F 代数无关，因此 $F(x)$ 关于 F 的超越次数是 1，显然 x 就是 $F(x)$关于 F 的代数底. 一般，F 的超越体 $F(x_1, \cdots, x_n)$关于 F 的超越次数是 n，并且 $x_1, \cdots, x_n$ 就是它关于 F 的代数底.

同 § 4.4 类似，假如 K 关于 F 的超越次数是 n，由 4，K 中任意 n 个关于 F 代数无关的元形成 K 关于 F 的代数底，再假如 $u_1, \cdots, u_m$ 是 K 关于 F 的代数底，那末 K 中任意元关于 F 与 $\{u_1, \cdots, u_m\}$代数相关，因此由 5，得知 K 中关于 F 代数无关的子集的元数不大于 m，于是我们有下面与 § 4.4 定理 2 类似的定理.

定理 2 K 关于体 F 的代数底的元数等于 K 关于 F 的超越次数.

我们知道在 F 的扩张体 K 中，除 F 中元外，如果没有 F 的代数元，那末 K 就叫做 F 的纯超越体. 添加 F 的超越元于 F 扩张的体当然是 F 的超越体，但它是否是 F 的纯超越体？

我们先来考虑超越单扩张体 $F(x)$. 因为其中任意元 u 是系数为 F 中元的 x 的有理函数，假如命 $u=\dfrac{f(x)}{g(x)}$，这里 $f(x)$，$g(x)$是 $F[x]$ 中互质的多项式，根据 § 3.9 定理 7，$f(x)$，$g(x)$除 F 中非零

元的因子外，由 u 一意决定．因此它们的次数也是由 u 一意决定，我们叫 $f(x)$，$g(x)$ 的次数中较大的做 u 关于 F 的**超越次数**．

定理 3　假定 u 是 F 的超越单扩张体 $F(x)$ 中关于 F 超越次数 $n>0$ 的元，那末 u 是 F 的超越元，并且 $F(x)$ 是 $F(u)$ 的 n 次代数体．

证明　假定 $u=\dfrac{f(x)}{g(x)}$，这里 $f(x)$，$g(x)$ 互质，因为 $ug(x)-f(x)=0$，所以 x 是 $F(u)[y]$ 中多项式 $h(y)=ug(y)-f(y)$ 的零点．但 $f(y)$，$g(y)$ 的次数都不大于 n，并且其中至少有一是 n，而 u 又不是 F 中元，因此 $h(y)$ 的次数是 n．假如我们还能够证明 $h(y)$ 是既约的，那末 x 是 $F(u)$ 的 n 次代数元，所以 $F(x)$ 是 $F(u)$ 的 n 次代数体．再因为 x 是 F 的超越元，所以 u 也是 F 的超越元．

假如 $h(y)$ 在 $F(u)[y]$ 中是可约的，那末它在 $F[u, y]$ 中也是可约的．因为 $h(y)$ 是 u 的 1 次式，所以它有一个只含 y 而不含 u 的因式，这因式显然就是 $f(y)$，$g(y)$ 的公因式，这与 $f(x)$，$g(x)$ 互质的假设不合，因此 $h(y)$ 在 $F(u)[y]$ 中是既约．这就是说 x 是 $F(u)$ 的 n 次代数元，于是定理成立．

特别当 $n=1$ 时，显然 $F(x)=F(u)$，这就是说，$F(x)$ 中任意关于 F 超越次数是 1 的元都是 $F(x)$ 关于 F 的本原元．显然，$F(x)$ 关于 F 的本原元也只能是这样的元，因此我们得知 u 是 $F(x)$ 关于 F 的本原元的必要充分条件是

$$u=\frac{ax+b}{cx+d},\quad ad-bc\neq 0.$$

因为在 $F(x)$ 中，除 F 中元外，任意元关于 F 的次数大于零，由定理 3，它是 F 的超越元，因此 $F(x)$ 是 F 的纯超越扩张体．一般我们有

定理 4　假定 $x_1, \cdots, x_n$ 是关于体 F 的未定元，那末 F 的超越体 $K=F(x_1, \cdots, x_n)$ 是 F 的纯超越体．

证明 我们用归纳法来证明．当 $n=1$ 时，定理成立．假定 $n-1$ 时定理成立，我们命 α 是 K 中关于 F 的任意代数元，因为 α 也是 $F(x_1, \cdots, x_{n-1})$ 的代数元，并且 K 是 $F(x_1, \cdots, x_{n-1})$ 的纯超越体，所以 $\alpha\in F(x_1, \cdots, x_{n-1})$．再由归纳法的假设，我们就有 $\alpha\in F$，这就是说，K 中 F 的任意代数元是 F 中元，因此 K 是 F 的纯超越体，所以定理成立．

假定可换体 K 是 F 的扩张体，$u_1, \cdots, u_n$ 是它关于 F 的代数底，那末 K 中任意元是 $F(u_1, \cdots, u_n)$ 的代数元，但 $F(u_1, \cdots, u_n)\cong F(x_1, \cdots, x_n)$，因此 $F(u_1, \cdots, u_n)$ 是 F 的纯超越体，于是我们得知 K 可以先自 F 纯超越扩张，然后再代数扩张而成．这与 §4.5 中任意扩张体可以先代数扩张再纯超越扩张而成的步骤恰相反．

最后我们介绍鲁洛斯(J. Lueroth, 1844～1910)定理，它在几何上还有重要的应用．

定理 5 假定 K 是可换体 F 的超越单扩张体 $F(x)$ 与 F 的中间体，并且异于 F，即 $F(x)\supseteqq K\supset F$，那末 K 是 F 的超越单扩张体．

证明 假定 u 是 K 中而不是 F 中的元，因为 x 是 $F(u)$ 的代数元，所以也是 K 的代数元，我们命

$$g(y)=y^n+a_1y^{n-1}+\cdots+a_n,\quad a_i\in K,$$

是 $K[y]$ 中 x 适合的既约多项式．因为 a_i 是 x 的有理函数，所以我们有 $k(x)\in F[x]$，使

$$f(x, y)=k(x)g(y)$$

是 $F[x, y]$ 中元，并且 $f(x, y)$ 写成 y 的多项式时，它的系数的最大公因式是 1，即 $f(x, y)$ 是 $K[y]$ 的本原多项式(§3.9)，$f(x, y)$ 对于 x 的次数假定是 m．

因为 $(K(x):K)=n$，而 $K(x)=F(x)$，所以 $(F(x):K)=n$．

假如 K 中有关于 F 超越次数是 n 的元 α，那末由定理 3，$(F(x):F(\alpha))=n$，但 $K\supseteqq F(\alpha)$，所以 $K=F(\alpha)$，这就是说，K 是 F 的超越单扩张体，因此定理就告成立。

因为 x 是 F 的超越元，所以 $g(y)$ 的系数 a_i 不能完全都是 F 中元，我们假定 a_j 不在 F 中，并且把 a_j 写成

$$\alpha=a_j=\frac{p(x)}{q(x)}=\frac{l(x)}{k(x)},$$

这里 $p(x)$ 与 $q(x)$ 互质。因为 $f(x,y)$ 对于 x 的次数是 m，所以 $l(x)$，$k(x)$ 的次数都不大于 m，因此 $p(x)$，$q(x)$ 的次数也都不大于 m。

再因为 $p(y)-\alpha q(y)$ 是 $K[y]$ 中 x 适合的多项式，所以它能被 $g(y)$ 整除，于是我们有

$$p(y)-\frac{p(x)}{q(x)}q(y)=r(x)v(y)g(y)$$

$$=\frac{r(x)}{s(x)k(x)}t(x,y)f(x,y),$$

因此

$$q(x)p(y)-p(x)q(y)=\frac{q(x)r(x)}{s(x)k(x)}t(x,y)f(x,y),$$

这里 $t(x,y)$ 与 $f(x,y)$ 一样都是 $K[y]$ 中本原多项式，由 §3.9 习题 5，我们得知两个本原多项式 $t(x,y)$，$f(x,y)$ 的乘积 $t(x,y)f(x,y)$ 仍是 $K[y]$ 的本原多项式，所以 $s(x)k(x)\mid q(x)r(x)$。因此

$$q(x)p(y)-p(x)q(y)=h(x,y)f(x,y),$$

$$h(x,y)\in F[x,y],$$

这时左边对于 x 的次数不大于 m，而右边 $f(x,y)$ 对于 x 的次数是 m，因此左边对于 x 的次数也是 m，所以 $h(x,y)$ 不含 x，于是右边没有是 $F[x]$ 中多项式的因式。假如 $h(x,y)$ 含 y，因为左边是 x，

y 的对称式，所以 x 的多项式 $h(y, x)$ 是它的因式，这与上面矛盾．因此 $h(x, y)$ 又不含 y，于是 $h(x, y)=h\in F$，因此

$$q(x)p(y)-p(x)q(y)=hf(x, y).$$

由 x, y 的对称性，我们得知 $f(x, y)$ 对于 y 的次数是 m，所以 $m=n$．因此 $p(x)$，$q(x)$ 中至少有一是 x 的 n 次多项式．于是 α 的超越次数是 n．所以定理得证．

由上面的证明，我们又知道 $g(y)$ 中不是 F 中元的系数都是 K 关于 F 的本原元．

把这定理与 § 4.8 定理 3 合并，我们就得到

定理 6 可换体 F 的任意单扩张体与 F 的中间体是 F 的单扩张体．

习 题 4.10

1．假定 K 关于 L 的超越次数是 m，L 关于 F 的超越次数是 n，试证 K 关于 F 的超越次数是 $m+n$．

2．假定 $\{u, v\}$ 关于 F 代数无关，试证 $\{u^3+v^2, v^2+u\}$ 关于 F 代数无关，并且

$$(F(u, v):F(u^3+v^2, v^2+u))=6.$$

3．怎样的对应是 $F(x)$ 不使 F 中任意元变动的自同构？

4．试用本节所述方法证明 § 4.4 定理 3．

参 考 文 献

[1] E. Steinitz, Algebraische Theorie der Körper, Herausges von R. Baer und H. Hasse, Berlin (1930).

[2] E. Snapper, Completely primary rings I, Ann. of Math., 52 (1950), 666~673; II, Ann. of Math., 53 (1951), 125~142; III, Ann. of Math., 53 (1951), 207~234; IV, Ann. of Math., 55 (1953), 46~64.

[3] A. A. Albert, Structure of algebras (1939).

[4] Slanozevic, Caslar, A sufficient and necessary condition for division rings, Bull. Soc. Math. Phys. Macédoine, 12 (1961), 25~29 (1963).

[5] R. W. Ball, A theorem on groups and the characteristic of an integral domain, Amer. Math. Monthly, 73 (1966), 1113.

[6] O. Zariski and P. Samual, Commutative Algebra, Vol. 1 (1958), 106~107.

[7] N. 贾柯勃逊著抽象代数(黄缘芳译),科学出版社,卷 2, 第九章, 215~216.

[8] A. A. Albert and H. Hasse, A determination of all normal division algebras over an algebraic number field, Trans. of Amer. Soc., 34 (1932), 722~726.

[9] Tsen C. C. (曾炯之), 1. Division Algebren über Funktionenkorper, Gott. Nach. (1933), 335~339.

——2. Algebren über Funktionenkörper, Gottin gen dissertation (1934).

[10] Lee H. C. (李华宗), 1. On Clifford's algebra, Jour. of London Math. Soc., 20 (1945), 27~32;

——2. On Clifford's algebras and their representation, Ann. of Math., 49 (1948), 760~773.

[11] (1) Report of a conference on linear algebras, Ram's Head Inn., Jane (1956), 6~8.

(2) R. D. Schafer, An introduction to nonassociative algebras (1966).

[12] I. N. Herstain, Finite multiplicative subgroups in division rings, Pacific Jour. of Math., 3 (1953), 121~126.

[13] (1) H. Goheen, The Wedderburn Theorem, Can. Jour. of Math., 7 (1955), 60~62.

(2) E. Witt, Über die Kommutativitätendlichen Schiefkörper, Abh. Math. Sem. Univ., Hamburg. 8 (1930), 413.

(3) I. N. Herstain, Wedderburn's theorem and a theorem of Jacobson, Amer. Math. Monthly, 68 (1961), 249~251.

[14] (1) N. Jacobson, Structure theory for algebraic algebras of bounded degree, Ann. of Math., 46 (1945), 695~707.

(2) Huzurbazar, M. S., Sivarama Hrishnan, K., Jacobson's theorem On commutativity of rings, Aligarh Bull. Math., 1 (1971), 9~12.

[15] (1) I. N. Herstain, 1. An elementary proof of a theorem of Jacobson, Duke Math. Jour., 21 (1954), 45~48.

——2. On a result of Faith, Canad. Math. Bull., 18, No. 4 (1975), 609.

(2) J. Luh, On the Commutativity of J-rings, Canadian J. of Math., 10 (1967), 1289~1292.

(3) Wansley, J. W., On a Condition for Commutativity of rings, J. London Math. Soc., (2) 4 (1971), 331~332.

[16] (1) I. N. Herstein, A condition for the commutativity of rings, Can. Jour. of Math., 9 (1957), 583~586.

(2) Tominaga, Hisao (富永久雄), A theorem on rings, Math. J. Okayama Univ., 9(1959), 9～12.
(3) Bell, Howard E, On some Commutativity Theorem of Herstein, Arch Math., 24 (1971), 34～38.

第五章

群　论

群的基本概念及基本性质在第二章已详细介绍，这章主要是讨论它的构造.

§5.1 算　子

由§4.4，我们知道向量空间是一个加群，它除了有它自身的加法结合法外，还有与另一集合的乘法结合法，现在我们根据这概念把§2.1中群的概念来推广．首先引入这个概念的是克努尔(W. Krull, 1889～)及诺特尔(E. Noether, 1882～1935).

定义1　假定G是群，M是集合，如果对于M中任意元λ，G中任意元a，b，

$$\lambda a\in G,\quad \lambda(ab)=\lambda a\cdot\lambda b,$$

那末λ叫做G的**(左)算子**，M叫做G的**(左)算子集**，G叫做**带(左)算集M的群**，有时又叫做**M-(左)群**，或简单地叫做**带算群**.

譬如任意整数n是可换群G的算子，这是因为，如果命$na=a^n$，那末由a，$b\in G$，我们就有$n(ab)=(ab)^n=a^nb^n=na\cdot nb$．再假如$R$是环，$\lambda$是其中一元，由$a$，$b\in R$我们有$\lambda a\in R$，$\lambda(a+b)=\lambda a+\lambda b$，所以$\lambda$是$R$看成加群时的一个算子.

我们容易知道群G的自同态是G的算子，因此任意群都有算子集，也就是说都可以看成带算群．象在第二章那样不考虑算子

集的群，我们可以说它的算子集是空集或者就是一个恒等同态.

假如 M 是群 G 的算子集，λ 是 M 中任意元，显然 $a\to\lambda a$ 是 G 的自同态，因此 M 中任意元可以看成为 G 的自同态，也就是说 M 是 G 的自同态集合. 根据同态的性质，我们得

$$\lambda e=e,\quad \lambda a^{-1}=(\lambda a)^{-1},\quad \lambda a^n=(\lambda a)^n.$$

假如群 G 的算子集是环 R，那末对于 R 中任意两元 u, v，根据 §3.3 环同态条件，我们要求

$$(u+v)a=ua+va,\quad (uv)a=u(va),\quad a\in G.$$

因此

$$(u-v)a=ua-va,\quad 0a=0.$$

如果 R 有单位元 e，我们还要求

$$ea=a,$$

也就是说，R 的单位元是 G 的**单位算子**. 于是整数环 Z 是可换群的算子集. 一个环是以自身做带算集的加群. §4.4 中讨论的 F 空间以及 F 的代数都是带算集 F 的加群.

假如 G 是带算集 M 的群，它的单位元群显然也是带算集 M 的群，但是 G 的其他子群不一定也是带算集 M 的群. 如果 G 的子群 H 是带算集 M 的群，也就是说，对于 M 中的任意元 λ，H 中任意元 h，

$$\lambda h\in H,$$

那末 H 叫做 G 的**带算子群**. 带算子群又是正规子群时，叫做**带算正规子群**.

群 G 的算子集假如是空集或者只是恒等同态，那末 G 的子群都是带算子群；假如是内同构群，那末它的带算子群都是正规子群；假如是自同构群，那末它的带算子群都是特征子群. 假如环看成是用自身做算子集的加群，那末它的带算子群就是它的左理想子环.

在 §2.3 中，我们得知可换群只有元数是 1 或者是质数时才是单群. 要注意的是，这性质对一般的带算群并不成立. 也就是说，一般带算可换单群的元数不一定是质数，譬如有理数体是以自身为带算集的加群，但它的元数不是质数.

我们很容易证明，两个带算子群的交以及由它们生成的子群都是带算子群.

在比较两个带算群，也就是在讨论两个带算群的同态、同构时，我们只考虑算子集是相同的情况. 由 §2.5，我们得知群的同态象是它的商群，因此我们要问，对于带算集 M 的群，它的怎样的商群也是带算集 M 的群，这时 M 与这商群的结合法又该怎样？

假如 H 是 G 的正规子群，λ 是 M 中任意元，如果 λ 又是商群 $\overline{G}=G/H$ 的算子，那末

$$\lambda H=H,$$

因此对于 H 中任意元 h，$\lambda h\in H$，所以 H 是 G 的带算正规子群. 再因为

$$\lambda(ah)=\lambda a\cdot\lambda h\in\lambda a\cdot H,\quad a\in G,\quad h\in H,$$

所以

$$\lambda(aH)\subseteq\lambda a\cdot H.$$

因此我们就有

$$\lambda\bar{a}=\overline{\lambda a}.$$

这就是说，λa 是 λa 所在的陪集. 根据这关系我们有

$$\lambda(\bar{a}\bar{b})=\lambda(\overline{ab})=\overline{\lambda(ab)}=\overline{\lambda a\cdot\lambda b}=\overline{\lambda a}\cdot\overline{\lambda b}=\lambda\bar{a}\cdot\lambda\bar{b}.$$

显然，这时 G 射到 $\overline{G}$ 上的同态 $a\to\bar{a}$ 具有性质

$$\lambda a\to\lambda\bar{a}.$$

引用这性质，我们可以把在第二章介绍的同构、同态等概念推广到带算群上面来.

定义 2 假如 G，G' 都是算子集为 M 的带算群，σ 是 G 射到

G' 上的同态，对于 M 中任意元 λ，当 $a\to a'=\sigma(a)$ 时，如果 $\lambda a\to\lambda a'$，也就是说

$$\sigma(\lambda a)=\lambda(\sigma(a)),\quad a\in G,$$

那末 σ 叫做 G 射到 G' 上的**带算集 M 的同态**，或简单地叫做**带算同态**，这时又叫 G, G' 是**带算同态**．带算同态映射是可逆映射时，叫做**带算同构**．

线性代数中，K 向量空间 V 的线性变换就是把 V 看成带算集 K 的加群时的带算自同态．

于是上面的 $a\to\bar{a}$ 就是 G 射到 $\bar{G}$ 上的带算同态．我们知道 G 的算子集中元可以看成 G 的自同态，由 $\sigma(\lambda(a))=\lambda(\sigma(a))$ 就有 $\sigma\lambda(a)=\lambda\sigma(a)$，因此 $\sigma\lambda=\lambda\sigma$，这就是说，$G$ 的带算同态能够与 G 的算子交换．

假如群的算子集是空集或者是恒等同态，那末它的子群都是带算子群，同构、同态也分别都是带算同构、带算同态．因此，§2.5 中定理就这种算子集说都一一成立．现在我们要问，在一般情形时是否也能如此？

假如 G, G' 是带算集 M 的群，σ 是 G 射到 G' 上的带算同态，E 是 G' 的单位元 e' 的完全象源，也就是带算同态核．因为 E 中任意元 $e_i\to e'$，那末

$$\lambda e_i\to\lambda e'=e',\quad \lambda\in M,$$

所以 $\lambda e_i\in E$，于是 E 是 G 的带算正规子群，因此 §2.5 的定理 2 这时也成立．又因为 $a\to\bar{a}$ 是 G 射到 $\bar{G}$ 上的带算同态，所以 §2.5 的定理 4、定理 5 这时都一一成立．

于是我们得知，当群是带算群时，只要子群、同构、同态等都是带算，那末 §2.5 中的定理都能够一一成立．此外，§3.3 的定理 1 这时也成立．但要注意，因为带算单纯加群不一定是元数是质数的循环群，所以它的同态环一般只是体而不是可换体．

为了简便，在后面我们把"带算"二字一律省去不写，说群就是指带算群，因此子群、同构、同态等也都是指带算的而言.

环对加法成群，因此对加法，它具备群的各性质，但这只考虑了加法而没有涉及另一个基本运算乘法，所以这样的性质不能显示环的特征．假如把环看成以自身为算子集的加群，这样既考虑了加法同时又考虑了乘法，得出的结果一般都是环的特性，因此带算群的理论在讨论环时是非常重要的.

要注意的是，环虽然可以看成以它的子集做算子集的带算加群，但是环的同态与带算加群的带算同态是有区别的．譬如假定 a 是环 R 中心的元，那末

$$r \to ra$$

是把 R 看成用它的任一子集做算子集的加群时的带算自同态，但不是环 R 的自同态.

下面是环的带算自同态的基本性质.

定理 1 假定 R 是有单位元 e 的环，τ 是把 R 看成以自身为(左)算子集的加群时的带算自同态，那末 R 中有唯一元 a 存在，使

$$\tau(r)=ra, \quad r \in R,$$

这就是说，R 的任意带算自同态与用 R 中某元右乘一致.

证明 假设 $\tau(e)=a$，因为 τ 是带算同态，所以

$$\tau(re)=r\tau(e)=ra,$$

因此 $\tau(r)=ra$．再假如 $\tau(r)=rb$，由 $ra=rb$，当 $r=e$ 时，即得 $a=b$．因此定理成立.

于是同 §3.3 习题 8 一样，我们容易证得

定理 2 假定 R 是有单位元的环，R' 是把 R 看成以自身为左算子集的加群的自同态环，那末 R 与 R' 逆同构.

同 §4.4 中一样，有时为了方便，我们把算子写在右边．写在

左边的叫做左群，写在右边的叫做右群．凡是左群的性质能够同样证明也是右群的性质．

一般，假如群 G 有左算子集 M，同时又有右算子集 N，这时如果它们中元又满足

$$(\lambda a)\mu=\lambda(a\mu),\quad a\in G,\quad \lambda\in M,\quad \mu\in N,$$

那末 G 叫做**带算集** M,N **的群**，或者叫做 M-N-**群**．当 $M=N$ 时，我们又叫 G 做 M **复群**．

由定义容易得知，μ 可以看成 M-左群 G 的带算自同态，λ 可看成 N-右群 G 的带算自同态，因此如果 M，N 都是乘集，那末 N 与 M-左群 G 的自同态群的子乘集逆同构，而 M 则与 N-右群 G 的自同态群的子乘集同构．

M-N-群 G 的子群如果又是 M-N-群，它就叫做 G 的**带算子群**．M-N-群 G 射到 M-N-群 G' 上的同态 σ，如果又满足

$$\sigma(\lambda a)=\lambda\sigma(a),\quad \sigma(a\mu)=\sigma(a)\cdot\mu,$$
$$\sigma(\lambda a\mu)=\lambda\sigma(a)\mu,$$

那末 σ 叫做**带算同态**．这时 §2.5 中定理及 §3.3 定理 1 都同样能够一一成立．

假如 R 是有单位元 e 的环，τ 是把 R 看成 R-复群时的带算自同态，因为 τ 也是把 R 看成以自身为左算子集加群时的带算自同态，由上面的定理 1，$\tau(r)=ra$．同样，因为 τ 又是把 R 看成以自身为右算子集加群时的带算自同态，所以

$$\tau(r)=\tau(er)=\tau(e)\cdot r=ar,$$

于是 $ra=ar$，这就是说，a 是 R 中与 R 的任意元能够交换的元，因此 a 在 R 的中心中．反过来，R 中心的任意元显然是 R 的带算自同态，于是 R 的带算自同态环与 R 的中心同构．

我们知道，单纯环有单位元时，它的中心是可换体（§3.6 习题 10），于是我们有与 §3.3 定理 1 类似的定理．

定理 3 有单位元的单纯环假如看成是自身的复群，那末它的带算自同态环是可换体.

同群一样，环也有所谓带算环，假如 R 是环，M 是集合，如果对于 M 中任意元 λ，R 中任意元 a, b,

$$\lambda a\in R,\quad \lambda(a+b)=\lambda a+\lambda b,\quad \lambda(ab)=(\lambda a)b=a(\lambda b),$$

那末 λ 叫做 R 的(左)算子，M 叫做 R 的(左)算子集，R 叫做带(左)算集 M 的环，有时又叫做 M-环，因此 F 的代数就是 F-环.

在讨论带算环时，我们就要考虑它的带算子环，带算理想子环以及带算同态、带算同构等，这些我们都不详细介绍了.

习 题 5.1

1. 试证带算同态把带算子群仍然变为带算子群.

2. 试证带算循环群的任意子群都是带算子群.

3. 在由有理数对 (a_1, a_2) 形成的环中(§3.1 习题 2)，由 $(1,0)$ 及 $(0,1)$ 生成的两个理想子环是看成环时的同构，但不是看成加群时的带算同构，这是为什么?

4. 假如把可换体 F 的 n 维向量空间 V 看成为带算集 F 的加群，试证 V 的自同态环与全矩阵环 F_n 同构.

§5.2 同构定理

在§2.5中我们介绍了一个同态基本定理，这节我们来介绍三个同构基本定理，它们在应用上都是很广泛的.

§2.5的定理5是 G' 的单位元群与它的完全象源的一个重要关系，下面的**第一同构定理**就是表示这种关系对于 G' 中任意正规子群也能够同样成立，因此第一同构定理可以说是表示两个同态群间商群的同构关系.

定理 1 假定 G, G' 是群，$G\sim G'$，H' 是 G' 的正规子群，那

末 H' 在 G 中的完全象源 H 是 G 的正规子群,并且

$$G/H \cong G'/H'.$$

证明 因为 $G \sim G'$, $G' \sim G'/H'$, 所以 $G \sim G'/H'$. 由第二个同态关系, 我们得知 G'/H' 的单位元在 G' 中的完全象源是 H'. 由假设, H' 在 G 中的完全象源是 H, 因此 G'/H' 的单位元在 G 中的完全象源就是 H, 也就是说 $G \sim G'/H'$ 时, 同态核是 H. 于是由 §2.5 定理 5, H 是 G 的正规子群并且 $G/H \cong G'/H'$, 因此定理得证.

上定理显然是 §2.5 定理 5 的推广,因为假如 $H'=e'$, 那末 E 就是 e' 的完全象源, G'/H' 就是 G'.

假如 $G \sim G'$, H 是 G 的正规子群, H' 是 H 在 G' 中的象,由同态对应关系,我们容易得知 H' 是 G' 的正规子群. 要注意的是,这时 H 不一定是 H' 的完全象源,因此 G/H, G'/H' 一般不是同构. 譬如假如 $a^{12}=1$, 由 $(a) \sim (a^2)$ 我们就有 $(a^4) \sim (a^4)$, 这时 $(a)/(a^4) \cong (a^3)$, $(a^2)/(a^4) \cong (a^6)$, 两者元数不同, 显然不同构. 但是它们是同态, 即

$$G/H \sim G'/H'.$$

这是因为, 我们把 G 分为 H 的陪集 a_iH, 因为 $(a_iH)'=a_i'H'$, 并且 $(a_ia_jH)'=a_i'a_j'H'$, 所以 $a_iH \to a_i'H'$ 是 G/H 射到 G'/H' 上的同态.

怎样的象源才是完全象源? 假定 $G \sim G'$, E 是它们的同态核, H' 是 G 的子群 H 在 G' 的象, H'' 是 H' 在 G 的完全象源. 因为 HE 的象是 H', 所以 $HE \subseteq H''$. 反过来, 因为 H'' 中任意元 k 与 H 中某元 h 在 G' 中有相同的象, 所以 $h^{-1}k$ 的象是单位元, 于是 $h^{-1}k \in E$, 即 $k \in hE$, 因此 $H'' \subseteq HE$, 所以 $H''=HE$. 这就是说, H'' 是 H 与同态核 E 的乘积 HE. 假如 $H \supseteq E$, 那末 H 就是 H' 的完全象源了.

假如 K, H 是群 G 的正规子群, 并且 $K\supseteq H$, 因为 $G\sim G/H$, 而 K 在 G/H 中的象是 K/H, 所以 K/H 是 G/H 的正规子群. 又因为 K/H 在 G 中的完全象源是 K, 由上面的定理 1, 我们有

$$G/K\cong G/H\Big/K/H. \tag{1}$$

下面是我们的**第二同构定理**, 它表示一个群中两个子群的积与它们的交之间的同构关系.

定理 2 假设 H 是群 G 的正规子群, K 是 G 的子群, 那末 $K\cap H$ 是 K 的正规子群, 并且

$$KH/H\cong K/K\cap H.$$

证明 假定 K 在 $\bar{G}=G/H$ 的象是 $\bar{K}$, 因为 $K\sim\bar{K}$, 并且同态核是 $K\cap H$, 所以 $\bar{K}\cong K/K\cap H$. 又因为 $G\sim\bar{G}$ 的同态核是 H, 而 $\bar{K}$ 在 G 的完全象源是 KH, 于是由 $KH\sim\bar{K}$, 我们就有 $\bar{K}\cong KH/H$, 因此定理成立.

譬如 $K=((1\,3\,2\,4))$, $H=B_4$ (§2.3), 因为

$KH=((1\,2),\ (1\,4)(2\,3))$, $K\cap H=\{(1),\ (1\,2)(3\,4)\}$,

由计算容易得知 KH/H 及 $K/K\cap H$ 都是元数是 2 的循环群, 所以它们同构.

特别, 当 $K\cap H$ 是单位元群时, 我们即得

$$KH/H\cong K,$$

也就是说, 这时我们简直可以把 H 消去.

下面**第三同构定理**, 是查生浩斯(H. Zassenhaus, 1912～)在 1934 年提出的, 也叫做**查生浩斯定理**, 它表示四个子群间的同构关系, 是第二同构定理的推广.

定理 3 假设 K, H 是群 G 的子群, K' 是 K 的正规子群, H' 是 H 的正规子群, 那末 $K'(K\cap H')$ 是 $K'(K\cap H)$ 的正规子

群，$H'(H\cap K')$ 是 $H'(H\cap K)$ 的正规子群，并且

$$K'(K\cap H)/K'(K\cap H')\cong H'(H\cap K)/H'(H\cap K').$$

证明 $K\cap H$ 及 $K'(K\cap H')$ 显然都是 $K'(K\cap H)$ 的子群．再 $K'(K\cap H')$ 又是 $K'(K\cap H)$ 的正规子群，这是因为，假如 $k'u$ 是 $K'(K\cap H)$ 中任意元，这里 $k'\in K'$, $u\in K\cap H$，那末

$$\begin{aligned}k'u\cdot K'(K\cap H')\cdot u^{-1}k'^{-1}&=k'K'\cdot u(K\cap H')u^{-1}k'^{-1}\\&\subseteq K'(K\cap H')k'^{-1}=K'k'^{-1}(K\cap H')\\&=K'(K\cap H').\end{aligned}$$

于是根据第二同构定理，我们有

$$\begin{aligned}&K'(K\cap H')(K\cap H)/K'(K\cap H')\\&\qquad\cong(K\cap H)/(K\cap H)\cap K'(K\cap H').\end{aligned}$$

显然 $(K\cap H')(K\cap H)=(K\cap H)$，假如我们能够证明

$$(K\cap H)\cap K'(K\cap H')=(K'\cap H)(K\cap H'),\tag{2}$$

那末
$$\begin{aligned}&K'(K\cap H)/K'(K\cap H')\\&\qquad\cong(K\cap H)/(K'\cap H)(K\cap H').\end{aligned}$$

因为在定理中，我们对于 K, K' 的要求，同对于 H, H' 的要求完全一样，假如在上式中把 K, K' 与 H, H' 互换，就得到

$$\begin{aligned}&H'(H\cap K)/H'(H\cap K')\\&\qquad\cong(K\cap H)/(K'\cap H)(K\cap H'),\end{aligned}$$

因此定理就告成立．

我们容易得知

$$(K'\cap H)(K\cap H')\subseteq(K\cap H),$$

$$(K'\cap H)(K\cap H')\subseteq K'(K\cap H'),$$

$$(K'\cap H)(K\cap H')\subseteq(K\cap H)\cap K'(K\cap H').$$

又假如 $a\in(K\cap H)\cap K'(K\cap H')$，那末 $a\in K\cap H$, $a\in K'(K\cap H')$，即 $a=k'u$, $k'\in K'$, $u\in K\cap H'$，因此 $k'\in H$，于是 $k'\in K'\cap H$，所以 $a\in(K'\cap H)(K\cap H')$，这就是说，

$$(K\cap H)\cap K'(K\cap H')\subseteq(K'\cap H)(K\cap H'),$$

于是(2)成立,因此定理得证.

特别,当 $K\supseteq H$,并且 H' 是单位元群时,我们就得到第二同构定理,因此第二同构定理是第三同构定理的特例.

我们知道,理想子环对于环与正规子群对于群相类似,在上面三个同构定理中,假如把群改为环,子群改为子环,正规子群改为理想子环,子群的积改为子环的和,那末这三个定理也都成立.

习 题 5.2

1. 试用第二同构定理证明对称群 S_4 关于 B_4 的商群与 S_3 同构.

2. 试证在由排列但不全是偶排列形成的群中,所有偶排列形成指标是2的正规子群.

3. 假如 H, K 是群 G 的子群,K' 是 K 的正规子群,试证 $H\cap K'$ 是 $H\cap K$ 的正规子群,并且 $H\cap K/H\cap K'$ 与 K/K' 的子群同构.

4. 试述关于环的第二同构定理并加证明.

5. 试证任意有穷体与多项式环 $Z[x]$ 对于某理想子环 N 的同余环 $Z[x]-N$ 同构.

§5.3 正规群列

在研究不是单群的群时,常常要考虑它的正规子群,因此常常引用由正规子群及正规子群的正规子群组成的正规子群列. 这节我们详细地讨论这种重要的子群列.

群 G 的有穷个子群 G_i 所成的子群列

$$(1)\qquad G=G_0\supset G_1\supset\cdots\supset G_k=E$$

叫做 G 的**正规群列**,k 叫做这正规群列的长,这里 E 是 G 的单位元群,G_i 是 G_{i-1} 的正规子群.

任意群除了单位元群外,显然都有正规群列. 譬如 $G\supset E$ 就

是 G 的正规群列．假如 G 不是单群，H 是异于 G 及 E 的正规子群，那末 $G\supset H\supset E$ 也是 G 的正规群列．

商群列

$$G/G_1,\quad G_1/G_2,\quad \cdots,\quad G_{k-1}/E$$

叫做正规群列(1)的**商群列**．一个群的两个正规群列，假如它们的长相等，依照某个顺序可以使第一个正规群列的商群与第二个正规群列的商群一一对一的对应，并且所对应的商群又都同构，那末这两个正规群列叫做**同构**．

譬如元数是 6 的循环群(a)的两个正规群列

$$(a)\supset(a^2)\supset E,\quad (a)\supset(a^3)\supset E$$

就是同构，这是因为它们的商群列都是由元数是 2 及 3 的两个循环群组成的．

假如

$$G=H_0\supset H_1\supset\cdots H_l=E \tag{2}$$

又是 G 的正规群列．如果 G 的正规群列(1)中任意子群 G_i 与(2)中某子群 H_j 相等，也就是说，(1)中任意子群都包含在(2)中，那末(2)叫做(1)的**加细**．显然这时 $k\leqslant l$．一个正规群列也可以看成是自身的加细．

一个群的任意两个正规群列显然不一定同构，下面我们来讨论(1)，(2)加细的同构．

首先我们来考虑(1)，(2)如何加细其长才相等，商群依怎样的顺序同构？因为(1)的长是 k，(2)的长是 l，假如我们在(1)中每二个子群 G_{i-1}，G_i 之间都插 $l-1$ 个子群 G_{ij}，在(2)中每二个 H_{j-1}，H_j 之间都插 $k-1$ 个子群 H_{ij}，即假如有

$$\begin{aligned}&G_{i-1}=G_{i0}\supseteqq G_{i1}\supseteqq\cdots\supseteqq G_{il}=G_i,\quad i=1,\ 2,\ \cdots,\ k,\\&H_{j-1}=H_{0j}\supseteqq H_{1j}\supseteqq\cdots\supseteqq H_{kj}=H_j,\quad j=1,\ 2,\ \cdots,\ l,\end{aligned}\tag{3}$$

那末这二个加细都包含 kl 个子群．再因为这时(1)的加细是 k 个

含有 l 个子群的组，(2)的加细是 l 个含有 k 个子群的组. 假如前者第 i 组的 l 个商群顺次与后者各组的第 i 个商群同构，即

$$(4) \qquad G_{ij-1}/G_{ij} \simeq H_{i-1j}/H_{ij},$$

那末上面这样的加细就是同构的了.

我们容易知道适合条件(4)的 G_{ij}, H_{ij}, 当然也适合条件(3)，但是怎样来挑选适合条件(4)的这些 G_{ij} 及 H_{ij} 呢？因为

$$G_{i-1} \supseteq G_{ij} \supseteq G_i, \quad H_{j-1} \supseteq H_{ij} \supseteq H_j,$$

我们可以取

$$G_{ij} = G_i K_{ij}, \quad K_{ij} \subseteq G_{i-1}; \quad H_{ij} = H_j L_{ij}, \quad L_{ij} \subseteq H_{j-1}.$$

因此条件(4)就是条件

$$G_i K_{ij-1}/G_i K_{ij} \simeq H_j L_{i-1j}/H_j L_{ij}.$$

显然根据第三同构定理，只要我们取

$$K_{ij} = G_{i-1} \cap H_j, \quad H_{ij} = H_{j-1} \cap G_i$$

就行了，也就是说，我们取

$$G_{ij} = G_i(G_{i-1} \cap H_j), \quad H_{ij} = H_j(H_{j-1} \cap G_i),$$

条件(4)就告成立.

再假如 $G_{ij-1} = G_{ij}$，那末 $G_{ij-1}/G_{ij} = E$，因此 $H_{i-1j} = H_{ij}$，反过来，如果 $H_{i-1j} = H_{ij}$，那末 $G_{ij-1} = G_{ij}$.

这就是说，把这样的 G_{ij} 插入 G_{i-1}, G_i 之间，删去相等的得到长不大于 kl 的(1)的加细与把 H_{ij} 插入 H_{j-1}, H_j 之间，删去相等的得到(2)的加细同构. 因此我们有下面**雪来义尔** (O. Schreier, 1901～1929) 定理.

定理 1 一个群的任意两个正规群列有同构的加细.

譬如 $G = (a)$ 是元数为 12 的循环群,

$$(a) \supset (a^2) \supset E, \quad (a) \supset (a^3) \supset E$$

是它的两个正规群列，这时

$$G_0 = H_0 = (a), \quad G_1 = (a^2), \quad H_1 = (a^3), \quad G_2 = H_2 = E,$$

于是我们有

$$G_{11}=G_1H_1=G_0,\ \ G_{21}=G_1\cap H_1=(a^6),$$
$$H_{11}=H_1G_1=H_0,\ \ H_{12}=H_1\cap G_1=(a^6).$$

因此

$$(a)\supset(a^2)\supset(a^6)\supset E,\ \ (a)\supset(a^3)\supset(a^6)\supset E$$

是上面两个正规群列的同构加细.

定义 1 一个正规群列如果没有异于它自身的加细，就叫做**合成群列**.

显然，有穷群是有合成群列的. 一个正规群列有时可以加细成为合成群列，譬如上面的$(a)\supset(a^2)\supset(a^6)\supset E$就是加细$(a)\supset(a^2)\supset E$所成的合成群列. 但也有不论如何加细终不能使它成为合成群列的,譬如$G=(a)$是无穷循环群,

$$G\supset G_1\supset\cdots\supset G_{k-1}\supset G_k=E$$

是它的任意正规群列,如果$G_{k-1}=(a^m)$,那末G_{k-1}, E之间还有正规子群(a^{2m})存在,所以这时不论如何加细不能使这正规群列成为合成群列. 这就是说，无穷循环群(a)没有合成群列，因此任一群不一定都有合成群列，一个正规群列也不一定都能够加细成为合成群列.

根据定理1，我们立即得到下面关于合成群列的两个主要定理.

定理 2 一个群的任意两个合成群列同构.

这定理叫做**约当-赫尔特尔定理**. 因此,一个群如果有合成群列,那末它的合成群列的长是一定的,这长又叫做这**群的长**.

定理 3 一个群如果有合成群列，那末它的任意正规群列都能够加细成为合成群列.

下面我们来讨论正规群列是合成群列的必要充分条件. 我们先介绍与§3.8中极大理想子环类似的重要概念以备引用.

假如G是群，H是它的正规子群，如果G中除G及H自身外，不再有包含H的正规子群，那末H就叫做G的**极大正规子群**. 譬如n个文字上的交代群A_n就是对称群S_n的极大正规子群. 假如H是G的正规子群，$\overline{G}=G/H$，如果H是极大正规子群，那末$\overline{G}$是单群. 这是因为，假如$\overline{G}$中有异于自身及单位元群的正规子群$\overline{K}$，因为$G\sim\overline{G}$，由第一同构定理，$\overline{K}$在G的完全象源K是G的正规子群，显然这时$G\supset K\supset H$，这与H是极大的假设不合. 反过来，假如$\overline{G}$是单群，因为同态把正规子群变为正规子群，所以G中除G及H外没有包含H的正规子群，因此H是极大正规子群. 于是我们得到

定理 4 群G的正规子群H是极大正规子群的必要充分条件是商群G/H为单群.

根据这定理，上面提出的问题不难立即解答.

假设(1)是G的正规群列，如果它是合成群列，那末G_i是G_{i-1}的极大正规子群，因此G_{i-1}/G_i是单群. 反过来，如果G_{i-1}/G_i是单群，那末G_i是G_{i-1}的极大正规子群，因此它就是合成群列. 于是我们有

定理 5 正规群列(1)是合成群列的必要充分条件是G_{i-1}/G_i $(i=1, \cdots, k)$是单群.

由约当-赫尔特尔定理，这些单群G_{i-1}/G_i由G一意决定.

引用正规群列，我们也可以把群来分类.

定义 2 群G假如它有商群都是可换群的正规群列，就叫做**可解群**.

显然，任意可换群都是可解群. 因为元数是质数的群是循环群，当然也是可换群，所以群的某正规群列中任意商群的元数如果都是质数，那末这个群就是可解群. 交代群A_5不是可解群，因为它是单群.

我们容易证明交代群 A_2, A_3, 对称群 S_2, S_3 都是可解群，又由 § 2.3, 得知

$$S_4 \supset A_4 \supset B_4 \supset C_4 \supset E, \quad C_4 = \{1, (12)(34)\}$$

是对称群 S_4 的正规群列，它的商群

$$S_4/A_4, \quad A_4/B_4, \quad B_4/C_4, \quad C_4$$

的元数分别是 2, 3, 2, 2，它们都是质数，所以 S_4 是可解群. 显然交代群 A_4 也是可解群，于是我们得知当 $n \leqslant 4$ 时，A_n, S_n 都是可解群.

由上例，我们又可以知道，虽然可换群是可解群，但可解群不一定是可换群. 此外我们还可以知道，可解群的任意正规群列的商群也不一定都是可换群. 譬如 S_4 的正规群列 $S_4 \supset E$ 的商群 S_4 就不是可换群. 但由定理 1 及上节的(1)式，我们能够加细使它成为商群都是可换群的正规群列，因此，如果可解群有合成群列，那末合成群列的商群都是可换单群.

我们知道 G 的换位子群是 $D(G)$，$D(G)$ 的换位子群我们就用 $D^2(G)$ 表示，因此 $D^{m+1}(G)$ 就是 $D^m(G)$ 的换位子群. 于是，假如 $D^k(G) = E$，由 § 2.3 定理 5，我们得知

$$G = D^0(G) \supset D(G) \supset \cdots \supset D^k(G) = E$$

是 G 的正规群列，并且它的商群都是可换群，因此这时 G 是可解群. 反过来，假如 G 是可解群，它的正规群列

$$G = G_0 \supset G_1 \supset \cdots \supset G_k = E$$

的商群 G_{i-1}/G_i 都是可换群，因为 G/G_1 是可换群，由 § 2.3 定理 5，G 的换位子群 $D(G) \subseteqq G_1$，又因为 G_1/G_2 是可换群，所以 $D(G_1) \subseteqq G_2$，但 $D^2(G) \subseteqq D(G_1)$，所以 $D^2(G) \subseteqq G_2$. 一般，我们有 $D^i(G) \subseteqq G_i$. 于是 $D^k(G) = E$. 因此我们得下面可解群的必要充分条件.

定理 6　群 G 是可解群的必要充分条件是有某正整数 k 存

在，使 $D^k(G)=E$，即 G 有正规群列

$$G=D^0(G)\supset D(G)\supset\cdots\supset D^k(G)=E.$$

因为当 $n\geqslant5$ 时，交代群 A_n 的换位子群仍然是它自身，所以不存在使 $D^k(A_n)=E$ 的 k，因此 $n\geqslant5$ 时，A_n 不是可解群.

下面是可解群的重要性质.

定理 7　可解群的子群是可解群.

证明　假定 H 是可解群 G 的子群，因为

$$D^k(H)\subseteq D^k(G)=E,$$

即 $D^k(H)=E$，所以 H 是可解群，于是定理成立.

因为当 $n\geqslant5$ 时，交代群 A_n 不是可解群，所以对称群 S_n 也不是可解群．于是我们得知 S_n，A_n，当 $n\leqslant4$ 时都是可解群，当 $n\geqslant5$ 时，都不是可解群.

定理 8　可解群的商群是可解群.

证明　假定 G 是可解群．$\overline{G}=G/H$ 是它的商群．因为 $G\sim\overline{G}$，又因为换位子的象是换位子，换位子的象源中也有换位子，所以 G 的换位子群 $D(G)$ 在 $\overline{G}$ 的象是 $\overline{G}$ 的换位子群 $D(\overline{G})$，因此

$$D(G)\sim D(\overline{G}).$$

但 $D^k(G)=E$，所以 $D^k(\overline{G})=\overline{E}$．于是 $\overline{G}$ 是可解群，因此定理成立.

最后，我们来介绍二类重要的可解群.

定理 9　p 群(§2.4 习题 6)是可解群.

证明　假定群 G 的元数是 p^n，我们对 n 用归纳法来证明.

当 $n=1$ 时，G 是循环群，显然这时定理成立．假定 C 是 G 的中心，因为 C 的元数大于1(§2.4 习题 6)，所以 $\overline{G}=G/C$ 的元数是 p^k，$k<n$．根据归纳法假设，$\overline{G}$ 是可解群．于是我们有 $D^k(\overline{G})=\overline{E}$，但 $G\sim\overline{G}$，而 $D^k(G)$ 的象是 $D^k(\overline{G})$，因此 $D^k(G)\subseteq C$．再因为 C 是可换群，当然也是可解群，于是我们又有 $D^l(C)=E$．因此

$$D^{k+l}(G) \subseteq D^l(C) = E,$$

即 $D^{k+l}(G)=E$，所以 G 是可解群，于是定理成立.

元数是 $p^a q^b$ (p, q 是不相等的质数)的群是可解群[2]，这是著名的勃恩散特(W. Burnside, 1852～1927)定理. 但元数是 $p^a q^b r^c$ 的群一般不是可解群，譬如 A_5 不是可解群，它的元数 $60=2^2\cdot3\cdot5$.

下面是范围较大的一类可解群.

假定 H 是群 G 的正规子群，那末由所有形状象

$$a^{-1}h^{-1}ah, \quad a\in G, \quad h\in H$$

的换位子生成的子群，我们用 $D[G, H]$ 来表示，显然 $D[G, G]=D(G)$. 因为 H 是 G 的正规子群，所以 $a^{-1}h^{-1}ah\in H$，因此 $D[G, H]\subseteq H$. 同 §2.3 中一样，对于任意 $g\in D[G, H]$，我们有 $aga^{-1}g^{-1}\in D[G, H]$. 于是 $aga^{-1}\in D[G, H]$，所以 $D[G, H]$ 是 G 的正规子群.

我们命 $D[G, G]=G_1$, $D[G, G_1]=G_2$, 一般 $D[G, G_{i-1}]=G_i$. 假如有某正整数 m 存在，使 $G_m=D[G, G_{m-1}]=E$，那末 G 叫做**幂零群**. 显然可换群是幂零群.

定理 10 幂零群是可解群.

证明 假定 G 是幂零群，$G_m=D[G, G_{m-1}]=E$，因为

$$D(G)=G_1, \quad D(G_1)=D[G_1, G_1]\subseteq D[G, G_1]=G_2,$$

所以 $D^2(G)=D(G_1)\subseteq G_2$，一般 $D^i(G)\subseteq G_i$，但 $G_m=E$. 所以 $D^m(G)=E$，于是 G 是可解群，因此定理得证.

1950 年华罗庚曾经证明非可换体的乘群不是可解群[3]. 1961 年怀特与汤卜生证明了元数是奇数的群都是可解群[4]，这是一个重要的结果.

与上面类似，对于环也有合成环列，即环 R 的子环列

$$R=R_0\supset R_1\supset\cdots\supset R_k=0,$$

其中 R_i 是 R_{i-1} 的极大理想子环，叫做环 R 的**合成环列**. 并且一个环的任意两个合成环列也同构，也就是说，R 的任意两个合成环列的项数相等，并且它们的同余环按某顺序彼此同构.

同样，体也有所谓合成体列. 体 K 的子体列

$$K=K_0\supset K_1\supset\cdots\supset K_l=F,\quad F\text{ 是质体},$$

其中 K_{i-1} 是 K_i 的正规扩张体，并且各体间不存在真中间正规扩张体时，叫做 K 的**合成体列**. 假如 K_{i-1} 关于 K_i 的次数是 n_i，那末

$$n_1,\ \cdots,\ n_l$$

叫做 K 的**次数列**. 当次数列中的数都是质数时，K 就叫做**可解体**.

习　题　5.3

1. 试证对称群 S_2, S_3 都是可解群.

2. 假如 G/H 是可解群，H 是可解群，那末 G 也是可解群.

3. 假如 H, K 都是群 G 的子群，并且 K 是正规子群，如果 H, K 都是可解群，那末 HK 也是可解群.

4. 假如 G 是群，试证 $D^k(G)$ 都是 G 的正规子群.

5. 假如 H, K 是群 G 的两个互异的极大正规子群. 试证 $G=HK$，并且

$$G/H\simeq K/H\cap K,\quad G/K\simeq H/H\cap K.$$

6. 试求对称群 S_4 的所有合成群列.

7. 假如可换群 G 有合成群列，那末 G 是有穷群.

8. 试证 $Q(\sqrt[4]{2}, i)$ 是可解体，这里 Q 是有理数体.

§ 5.4　直　　积

在群论中，直积是一个重要概念，它把一个群用构造比它简单的子群来表达，在讨论群的构造时起着重大作用，这节介绍它的基本概念及基本性质.

由§2.3我们知道，假如群G是它的两个子群A，B的乘积，即$G=AB$，那末G中任意元能够用ab，$a\in A$，$b\in B$来表示．但是这表示一般不是一意的，并且G的结合法不一定能够用A，B的结合法来完全决定．如果A，B满足某些条件，这要求是可以达到的．这样我们就有了直积这个概念．

假定A，B是群G的子群，如果

1° A，B都是正规子群；

2° $G=AB$；

3° $A\cap B=E$，E是G的单位元群．

那末G叫做子群A，B的**直积**，用记号$G=A\times B$来表示．这时我们又说G能够分解为A，B的直积，A，B叫做G的**直积因子**．

譬如6元循环群(a)是子群(a^2)，(a^3)的直积，即

$$(a)=(a^2)\times(a^3).$$

这概念我们又常常用下面另一形式来表达．

假设A，B是群G的子群，如果

1° G中任意元g能够一意地表为

$$g=ab,\quad a\in A,\quad b\in B;$$

2° A中任意元与B中任意元能够交换，

那末G叫做A，B的直积．

下面我们来证明这两个概念是一致的．

假如根据第一个定义，G是它的子群A，B的直积，因为对于G中任意元g，我们有$g=ab$，如果

$$g=a_1b_1=a_2b_2,\quad a_1,\ a_2\in A,\quad b_1,\ b_2\in B,$$

那就有$a_2^{-1}a_1=b_2b_1^{-1}$．但$A\cap B=E$，于是

$$a_2^{-1}a_1=b_2b_1^{-1}=e,\quad e\text{ 是 }G\text{ 的单位元},$$

所以$a_1=a_2$，$b_1=b_2$．因此$g=ab$这种表示是一意的．再因为A，B都是G的正规子群，所以

$$aba^{-1}b^{-1}=a(ba^{-1}b^{-1})=(aba^{-1})b^{-1}$$

是 A 中元，同时也是 B 中元，于是

$$aba^{-1}b^{-1}=e,$$

所以 $ab=ba$，因此 A 中任意元与 B 中任意元能够交换，所以这时根据第二个定义，G 也是 A，B 的直积.

反过来，假如根据第二个定义，G 是子群 A、B 的直积，因为对于 G 中任意元 g，我们有 $g=ab$，所以 $G\subseteq AB$. 因此 $G=AB$. 又因为 A 中任意元与 B 中任意元能够交换，所以

$$gAg^{-1}=abAb^{-1}a^{-1}=aAa^{-1}\subseteq A,$$

因此 A 是 G 的正规子群. 同样 B 也是 G 的正规子群. 再假如 $c\in A\cap B$，那末

$$c=c\cdot e=e\cdot c.$$

因为这种表示是一意的，所以 $c=e$，于是 $A\cap B=E$，因此这时根据第一个定义，G 也是 A，B 的直积. 所以两个直积概念是一致的.

假如 G 是子群 A，B 的直积，g_1，g_2 是 G 中任意元，

$$g_1=a_1b_1,\quad g_2=a_2b_2,$$

那末

$$g_1g_2=a_1a_2\cdot b_1b_2.$$

这就是说，G 中任意两元相乘，只要乘它们的因子就行了. 因此，假如 A，B 的构造已经知道，那末 $G=A\times B$ 的构造也就知道，也就是说，G 能够由 A，B 一意决定. 当 G 是有穷群时，G 的元数是 A 的元数与 B 的元数的乘积.

由定义我们容易得知，假如 $G=A\times B$，显然 $G=B\times A$. 再根据第二同构定理，我们有

$$A\cong G/B,\quad B\cong G/A.$$

这就是说，假如 $G=A\times B$，那末 A 是 $G\sim G/A$ 的同态核，并且这同态又是 B 与 G/A 的同构. 因此 G 是与它的同态象同构的子群

与同态核的直积. 反过来, 假如 A 是群 G 的某同态的同态核, 并且这同态又是同态象与 G 的正规子群 B 的同构, 那末 $G=A\times B$. 这是因为, G 中任意元与 B 中某一元在 A 的同一陪集, 所以 $G=AB$. 再因为 $B\cong G/A$, 所以 $A\cap B=E$, 因此 G 是 A, B 的直积.

当 G 是加群时, 如果 G 是 A, B 的直积, 我们就用 $G=A+B$ 来表示, 叫 G 做 A, B 的**直和**, A, B 叫做 G 的**直和因子**.

上面两个子群直积的概念, 我们可以把它来推广.

假设 $A_1, A_2, \cdots, A_n$ 是群 G 的子群, 如果

1° $A_1, A_2, \cdots, A_n$ 都是 G 的正规子群;

2° $G=A_1A_2\cdots A_n$;

3° $B_i\cap A_i=E$, $B_i=A_1\cdots A_{i-1}$, $i=2, \cdots, n$, E 是 G 的单位元群.

那末 G 叫做 $A_1, A_2, \cdots, A_n$ 的**直积**, 即 $G=A_1\times A_2\times\cdots\times A_n$, 而 A_i 叫做 G 的**直积因子**.

同上面的讨论一样, 假如 G 是 $A_1, \cdots, A_n$ 的直积, 容易得知

1. G 中任意元 g 能够一意地表为

$$g=a_1a_2\cdots a_n,\quad a_i\in A_i.$$

2. A_i 中任意元与 $A_j(i\neq j)$ 中任意元能够交换.

并且这是直积定义的另一种表达形式, 这是因为, 假如根据这定义, G 是子群 $A_i(i=1, 2, \cdots, n)$ 的直积, 命

$$B_i'=A_1\cdots A_{i-1}A_{i+1}\cdots A_n,$$

那末

$$G=A_i\times B_i'.$$

于是 A_i 是 G 的正规子群, 并且因为 $A_i\cap B_i'=E$, 所以 $A_i\cap B_i=E$, 因此根据上面的定义, G 也是 A_i 的直积, 这就是说, 上面的定义能够由这定义推出.

要注意的是, 假如 G 中任意元能够表为 $A_i(i=1, 2, \cdots, n)$ 中

元的乘积，并且 A_i 中任意元与 $A_j(i\neq j)$ 中任意元又能够交换，这时只要对于 G 的单位元 e 这种表示是一意的，那末对于 G 中任意元这种表示也是一意的．这是因为，如果

$$a_1a_2\cdots a_n=a_1'a_2'\cdots a_n',$$

我们就有 $a_1'a_1^{-1}a_2'a_2^{-1}\cdots a_n'a_n^{-1}=e$，因此 $a_i'=a_i(i=1,\ 2,\ \cdots,\ n)$．

上面是介绍直积的概念，现在我们来讨论直积的性质．

假如 $G=A_1\times A_2\times\cdots\times A_n$，如果

$$A_1'=A_1\times\cdots\times A_{n_1},\quad A_2'=A_{n_1+1}\times\cdots\times A_{n_1+n_2},\quad\cdots,$$
$$A_m'=A_{n_1+\cdots+n_{m-1}+1}\times\cdots\times A_n,$$

那末我们有

(1)
$$G=A_1'\times A_2'\times\cdots\times A_m'.$$

如果 $A_i=B_{i1}\times\cdots\times B_{im_i}$，由定义我们又容易验证

$$G=B_{11}\times\cdots\times B_{1m_1}\times\cdots\times B_{n1}\times\cdots\times B_{nm_n},$$

这就是说，在若干个子群的直积中，与元素乘积的情况一样，我们可以任意添加括弧或减少括弧．

假如 $G=A_1\times A_2\times\cdots\times A_n$，命 $G_i=A_1\times\cdots\times A_{n-i}(i=0,\ \cdots,\ n)$，我们就得到 G 的正规群列

(2)
$$G=G_0\supset G_1\supset\cdots\supset G_n=E.$$

这时如果 $G_{i-1}/G_i\cong A_{n-i+1}$ 有合成群列，命

$$A_i=A_{i0}\supset A_{i1}\supset\cdots\supset A_{ik_i}=E$$

是 A_i 的合成群列，于是我们有

(3)
$$G_{n-i}=G_{n-i+1}A_{i0}\supset G_{n-i+1}A_{i1}\supset\cdots\supset G_{n-i+1}A_{ik_i}=G_{n-i+1},$$

由第一同构定理，我们容易得知 $G_{n-i+1}A_{ij}$ 是 $G_{n-i+1}A_{ij-1}$ 的正规子群，并且

$$G_{n-i+1}A_{ij-1}/G_{n-i+1}A_{ij}\cong A_{ij-1}/A_{ij},$$

因此 $G_{n-i+1}A_{ij-1}/G_{n-i+1}A_{ij}$ 是单群，于是上面的正规群列(2)用(3)加细就得到 G 的合成群列．就是说，假如 $G=A_1\times A_2\times\cdots\times A_n$，

如果A_i都有合成群列，那末G也有合成群列，并且G的长等于A_i的长的和.

假定V是体F的向量空间，因为V是带算集F的加群，如果它有由n个元形成的关于F的底，那末V的长是n，因此由§5.3约当-赫尔特尔定理，n是一意的. 这就是说，V关于F的底的元数是一定的. 但是V中任意$(V:F)$个关于F线性无关的元形成它的底，所以V关于F的底的元数等于$(V:F)$，这就是§4.4中定理3不需要其中定理1、定理2的另一证明.

假如G是群，

$$G=A\times B=A_1\times B_1,$$

如果$B\cong B_1$时，

$$A\cong A_1,$$

我们就说B能够从直积中消去. 假如G是有穷循环群，显然B可以从直积中消去. 1962年卡普伦斯基(I. Kaplansky)猜测当B是无穷循环群时，B也可以从直积中消去. 1967年胡柯(L. Fuchs)证明无穷循环群不能从直积中消去，否认了这个猜测. 1969年伊桑(R. Hirshon)证明了当B是有穷群时，它可以从直积中消去；当B是无穷群时，如果它满足正规子群的极大条件，也可以从直积中消去，解答了这问题. 1975年伊桑对这又有新结果，读者欲知其详，请参考文献[5].

一个群假如能够分解为真子群的直积，它的子群不一定也都能够分解为真子群的直积，但是它的某些子群却能够如此.

定理1　假设群$G=A\times B$，H是G的子群，并且$H\supseteq A$，那末

$$H=A\times(H\cap B).$$

证明　因为$H\subseteq G$，所以H中任意元h可以写成

$$h=ab,\quad a\in A,\quad b\in B.$$

但 $b=a^{-1}h\in H$, 因此 $b\in H\cap B$, 所以

$$H=A(H\cap B).$$

再因为 A, B 是 G 的正规子群，所以 A, $H\cap B$ 都是 H 的正规子群，又因为

$$A\cap(H\cap B)\subseteq A\cap B=E,$$

所以 H 是 A, $H\cap B$ 的直积，因此定理得证.

一个群如果能够分解为它的真子群的直积，就叫做**可约群**，否则叫做**既约群**. 譬如对称群 S_n 就是既约群 (§2.3 习题 10, 11). 再元数是质数幂的循环群以及无穷循环群也都是既约群. 这是因为，它们的任意两个子群的交都异于单位元群. 一个群如果能够分解为它的真子单群的直积，就叫做**完全可约群**.

我们很容易知道，假如 G 是完全可约群，它分解为 n 个单群的直积，那末它有长是 n 的合成群列，也就是说它的长是 n.

下面是完全可约群的基本性质.

定理 2 假设 G 是完全可约群，A 是它的任意正规子群，那就有一正规子群 B 存在，使得 G 是 A, B 的直积，即

$$G=A\times B.$$

这就是说，完全可约群的任意正规子群是它的直积因子.

证明 假设 $G=A_1\times\cdots\times A_n$, A_i 是单群，那末

$$G=A\cdot A_1\cdots A_n.$$

因为 A_1 是单群，$A\cap A_1$ 是 A_1 的正规子群，所以 $A\cap A_1$ 是 A_1 或者是单位元群 E. 当 $A\cap A_1=A_1$ 时，$AA_1=A$, 这时我们把 A_1 删去；当 $A\cap A_1=E$ 时，$AA_1=A\times A_1$, 这时我们把 AA_1 改写成 $A\times A_1$. 这样继续进行，一般因为 $(A\cdot A_1\cdots A_{k-1})\cap A_k$ 是单群 A_k 的正规子群，所以它是 A_k 或 E, 因此我们可以把 A_k 删去或把 $(A\cdot A_1\cdots A_{k-1})A_k$ 改写成 $(A\cdot A_1\cdots A_{k-1})\times A_k$. 假如把所有这些多余的 A_i 一一删去，把剩下的乘积改成直积，我们就得到

$$G=A\times A_{i_1}\times\cdots\times A_{i_r},$$

因此 $A_{i_1}\times\cdots\times A_{i_r}$ 就是所求的正规子群 B, 所以定理得证.

在上面的证明中, 假如把 $G=A_1\times\cdots\times A_n$ 中异于 $A_{i_1}, \cdots, A_{i_r}$ 的直积因子的直积用 A' 表示, 那末 $G=A'\times A_{i_1}\times\cdots\times A_{i_r}$, 因此 $A\simeq A'$. 但 A' 是完全可约群, 所以 A 也是完全可约群. 再假如 A 是完全可约群 G 的正规子群, 由 $G=A\times B$, 我们有 $G/A\simeq B$. 因为 B 是 G 的正规子群,所以是完全可约群, 因此 G/A 是完全可约群. 于是我们有

定理 3 完全可约群的正规子群是完全可约群. 完全可约群的商群也是完全可约群.

由 §2.3, 我们知道在一般群中, 正规子群这个关系是不适合传递律的,但在完全可约群中, 传递律能够成立. 这是因为, 完全可约群的正规子群是它的直积因子. 再由定义我们容易证明, 任意直积因子的正规子群仍然是群的正规子群. 因此, 假如 G 是完全可约群, 如果 A 是 B 的正规子群, B 又是 G 的正规子群, 那末 A 是 G 的正规子群.

在 §3.9, 我们讨论了元素的分解, 这里我们介绍群的分解. 一个群在什么条件下能分解为既约群的直积, 在什么条件下这种分解又是一意的? 对此, 克努尔, 雷马克 (R. Remark), 许密特 (E. Schmidt, 1845~1921) 有一个重要定理[6], 这里不多谈了.

上面是讨论在同一群中若干个子群的直积, 任意若干个群的直积我们也可以仿照上面的方法来定义.

假定 A, B 是两个群(相等或不相等), 我们取所有元素对

$$(a, b),\quad a\in A,\quad b\in B,$$

并且规定

$$(a_1, b_1)=(a_2, b_2),\ 当\ a_1=a_2,\ b_1=b_2,$$

$$(a_1, b_1)\cdot(a_2, b_2)=(a_1a_2, b_1b_2),$$

那末所有这样的元素对形成为群 G，其中所有形状象 (a, e) 及 (e, b) 的元素对分别形成与 A, B 同构的子群 A', B'，这里 e 是 A, B 中的单位元. 显然 A', B' 是 G 的正规子群. 根据直积定义，我们容易证明 G 是子群 A', B' 的直积，这时我们把 A', B' 分别看成 A, B, 因此 G 就是 A, B 的直积，即 $G=A\times B$.

显然，当 A, B 都是可换群时，$G=A\times B$ 也是可换群. 假如我们把 (a, b) 与 (b, a) 对应，即 $(a, b)\rightarrow(b, a)$，那末这对应就是 $A\times B$ 射到 $B\times A$ 上的同构，因此 $A\times B\cong B\times A$. 再因 $((a, b), c)\rightarrow(a, (b, c))$ 是 $(A\times B)\times C$ 射到 $A\times(B\times C)$ 上的同构，于是 $(A\times B)\times C\cong A\times(B\times C)$，所以我们又有

$$A\times B=B\times A, \quad (A\times B)\times C=A\times(B\times C),$$

即直积因子适合乘法的交换律及结合律.

为了方便，我们又常常把 (a, b) 写成普通乘积的形状 ab，即

$$(a, b)=ab,$$

因此 $\qquad a_1b_1=a_2b_2$, 当 $a_1=a_2$, $b_1=b_2$,

并且 $\qquad (a_1b_1)(a_2b_2)=(a_1a_2)(b_1b_2)$.

关于 n 个群 $A_1, \cdots, A_n$ 的直积，我们可以根据

$$A_1\times\cdots\times A_{n-1}\times A_n=(A_1\times\cdots\times A_{n-1})\times A_n$$

用归纳法来定义.

与群的直积类似，我们有环的直和.

假定 $R_1, R_2, \cdots, R_n$ 是 n 个环，那末所有形状象 $(a_1, \cdots, a_n)$, $a_i\in R_i$, 的元根据下面规定的结合法：

$$(a_1, \cdots, a_n)=(a_1', \cdots, a_n'), \text{ 当 } a_i=a_i' \quad (i=1, 2, \cdots, n),$$

$$(a_1, \cdots, a_n)+(a_1', \cdots, a_n')=(a_1+a_1', \cdots, a_n+a_n'),$$

$$(a_1, \cdots, a_n)\cdot(a_1', \cdots, a_n')=(a_1a_1', \cdots, a_na_n'),$$

形成一个环 R，其中所有形状象 $(0, \cdots, a_i, \cdots, 0)$, $a_i\in R_i$, 的元形成与 R_i 同构的子环，这 R 我们就叫做它的子环 $R_1, \cdots, R_n$ 的直

和，用 $R=R_1+\cdots+R_n$ 表示．显然这时 $R_1,\cdots,R_n$ 是 R 的理想子环．我们也常常把 $(a_1,\cdots,a_n)$ 写成和的形状 $a_1+\cdots+a_n$，即 $(a_1,\cdots,a_n)=a_1+\cdots+a_n$．

假如环 R 看成加群时是它的理想子环 R_i，$i=1,\cdots,n$，的直和．那末环 R 也是子环 R_i 的直和．这是因为加群 R 是子加群 R_i 的直和，所以上面的规定中前两个条件成立．再因为 R_i 是 R 的理想子环，所以由 $R_i\cap R_j=0$，我们就有 $R_iR_j=0$，$i\neq j$．于是

$$(a_1+\cdots+a_n)\cdot(a_1'+\cdots+a_n')=a_1a_1'+\cdots+a_na_n',\quad a_i,\ a_i'\in R_i,$$

即上面第三个条件也成立．因此 $R=R_1+\cdots+R_n$．

同群的情况一样，$R=R_1+\cdots+R_n$ 时，R 中元能够一意地表为 $R_1,\cdots,R_n$ 中元的和，再 R 的结合法能够由 R_i 的结合法一意决定．因此引用直和，一个环可以化为构造比它简单的环来研究．譬如 $Z-(6)$ 显然不是体，但它是体 $Z-(2)$，$Z-(3)$ 的直和，即 $Z-(6)=(Z-(2))+(Z-(3))$．又 R_i 的理想子环也是 R 的理想子环．此外，在若干个子环的直和中，我们也可以任意增加或减少括弧．

一个环假如不能分解为真子环的直和，就叫做**既约环**．显然，单纯环是既约环，质环也是既约环．

下面两个性质与定理 1、定理 2 类似，不是一般环所具备的．

与定理 2 类似，我们有

定理 4　假如 $A\neq R$ 是环 R 中有单位元的理想子环，那末 R 是 A 及另一理想子环 B 的直和．

证明　假定 e 是 A 的单位元，那末 R 中所有适合 $re=0$，$er=0$ 的元 r 形成 R 的理想子环 B，显然 $A\cap B=0$．再假如 r 为 R 中任意元．因为 $(re)e=re\in A$，命 $re=a$ 即得 $re=ae$，于是 $(r-a)e=0$．再因为 e 是 A 的单位元，$er\in A$，所以 $ere=er$，即 $e(r-a)=0$．因此 $r-a\in B$．命 $r-a=b$，我们有 $r=a+b$．于是

R 看成加群时是 A, B 的直和，即 $R=A+B$, 所以定理成立。

此外我们还有与定理 1 类似的

定理 5 假如 R 是有单位元 e 的环，并且是子环 $R_1, \cdots, R_n$ 的直和，即 $R=R_1+\cdots+R_n$, 如果 L 是 R 的左理想子环，那末

$$L=L_1+\cdots+L_n,$$

这里 $L_i=R_i\cap L$.

证明 首先因为 R_i 都是 R 的理想子环，并且 $L\subseteq R$, 所以 L 都是 L 的理想子环. 再因为

$$e=e_1+\cdots+e_n,\quad e_i\in R_i,$$

所以对于 L 中任意元 a, 我们有

$$a=ea=e_1a+\cdots+e_ra.$$

由于 $a\in L\subseteq R$, 所以 $e_ia\in R_iR=R_i$; 又由于 $e_i\in R_i\subset R$, 所以 $e_ia\in RL=L$. 于是 $e_ia\in R_i\cap L=L_i$, 这就是说，L 中任意元能够表为它的理想子环 $L_1, \cdots, L_n$ 中元的和. 但 R 是 $R_1, \cdots, R_n$ 的直和，而 $L_i\subseteq R_i$, 所以 L 中元能够一意地表为 $L_1, \cdots, L_n$ 中元的和，因此 L 是 L_i 的直和. 于是定理成立.

要注意的是，上定理中 R 是有单位元的环，假如 R 没有单位元，定理是不成立的. 譬如设 $Z-(8)=\{\bar{0}, \bar{1}, \cdots, \bar{7}\}$ 中子环 $R_1=\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$, 那末 $L=\{(\bar{0}, \bar{0}), (\bar{4}, \bar{4})\}$ 是 $R=R_1+R_1$ 的理想子环，但它不是 R_1 的理想子环的直和.

习 题 5.4

1. 假设 (a) 是元数 $n=rs$ 的循环群，其中 $(r, s)=1$, 试证 (a) 是元数为 r 的循环群 (a^s) 与元数为 s 的循环群 (a^r) 的直积.

2. 假如循环群 A, B 的元数分别为 m, n, 试证 $A\times B$ 是循环群的必要充分条件是 m, n 互质，即 $(m, n)=1$.

3. 试求两个 3 元群的直积.

4. 假如 H 是可换群 G 的子群，G/H 是无穷循环群，试证

$$G=H\times G/H.$$

5. 假设 A, B 是群 G 的正规子群，$G=AB$, $H=A\cap B$，试证

$$G/H\cong A/H\times B/H.$$

6. 假如 A, B 是群 G 的正规子群，试证

$$AB\text{ 的长}+A\cap B\text{ 的长}=A\text{ 的长}+B\text{ 的长}.$$

7. 假如环 R 是它的子环 R_i, $i=1, \cdots, n$, 的直和，即 $R=R_1+\cdots+R_n$，那末 R_i 是 R 的理想子环.

8. 假设环 $R=R_1+\cdots+R_n$, C, C_i 分别是 R, R_i 的中心，试证

$$C=C_1+\cdots+C_n.$$

9. 假如环 R 看成加群时是它的左理想子环 $R_1, \cdots, R_n$ 的直和，R 的单位元

$$e=e_1+\cdots+e_n,\quad e_i\in R_i,$$

那末 e_ie_j, 当 $i=j$ 时为 e, 当 $i\neq j$ 时为 0.

10. 假如环有异于单位元的幂等元，那末这环为以此幂等元为单位元的理想子环与其他理想子环的直和.

§ 5.5 可 换 群

这节我们讨论可换群的构造，也就是讨论可换群如何一意地分解为既约群(循环 p 群，无穷循环群)的直积，这里所说的群都是可换群. 我们先从较简单的 p 群开始.

定理 1 p 群能够分解为循环 p 群的直积.

证明 假定 G 的元数是 p^n, 我们对 n 用归纳法来证明.

$n=1$ 时，定理显然成立. 假定 $n-1$ 时定理成立，下面我们来证明 n 时定理也成立.

假定 a 是 G 中阶数 p^r 最大的元，那末 $\overline{G}=G/(a)$ 的元数 $\dfrac{p^n}{p^r}=p^{n-r}$，因此 $\overline{G}$ 也是 p 群. 于是根据归纳法假设就得到

$$\overline{G}=(\overline{a}_1)\times\cdots\times(\overline{a}_m). \tag{1}$$

下面我们来证明 $G=(a)\times(a_1)\times\cdots\times(a_m)$，这里 a_i 是 $\bar{a}_i$ 在 G 的某个象源．显然 a_i 的阶数都是 p 的幂，因此定理就告成立．

首先，对于 G 中任意元 g，由 $\bar{g}\in\bar{G}$，得

$$\bar{g}=\bar{a}_1^{r_1}\cdots\bar{a}_m^{r_m}=\overline{a_1^{r_1}\cdots a_m^{r_m}},$$

因此

$$g=a^{r}a_1^{r_1}\cdots a_m^{r_m},$$

这就是说，g 是 (a)，(a_1)，$\cdots$，(a_m) 中元的乘积．

再假如 $a^s a_1^{s_1}\cdots a_m^{s_m}=e$，因为 $\bar{a}$ 是 $\bar{G}$ 的单位元，即 $\bar{a}=\bar{e}$，所以 $\bar{a}_1^{s_1}\cdots\bar{a}_m^{s_m}=\bar{e}$，由 (1) 我们有

(2) $$\bar{a}_i^{s_i}=\bar{e},\quad i=1,\ \cdots,\ m.$$

我们命 $\bar{a}_i$ 的阶数是 p^{t_i}，a_i 的阶数是 $p^{t_i'}$，显然 $t_i'\geqslant t_i$．如果 $t_i'=t_i$，也就是说，a_i 的阶数也是 p^{t_i}，由 (2) 我们有 $p^{t_i}|s_i$，于是 $a_i^{s_i}=e$，因此 $a^s=e$，根据定义 $G=(a)\times(a_1)\times\cdots\times(a_m)$，所以这时定理成立．如果 $t_i'\neq t_i$，因为 $\bar{a}_i$ 的象源 a_i 不是唯一的，假如我们能够另选 a_i' 代替 a_i，使 a_i' 的阶数为 p^{t_i}，即 a_i' 的阶数与 $\bar{a}_i$ 的阶数相等，那末 $G=(a)\times(a_1')\times\cdots\times(a_m')$，因此定理也同样成立．我们知道

$$\overline{a_i^{p^{t_i}}}=\bar{a}_i^{p^{t_i}}=\bar{e},$$

因此 $a_i^{p^{t_i}}\in(a)$，我们命 $a_i^{p^{t_i}}=a^{\lambda}$，$\lambda$ 是整数，由

$$a^{\lambda p^{r-t_i}}=(a_i^{p^{t_i}})^{p^{r-t_i}}=a_i^{p^r}=e,$$

我们就得到 $p^r|\lambda p^{r-t_i}$，即 $\lambda=\mu p^{t_i}$．命 $a_i'=a_i a^{-\mu}$，那末

$$a_i'^{\,p^{t_i}}=a_i^{p^{t_i}}a^{-\mu p^{t_i}}=e,$$

所以 a_i' 的阶数是 p^{t_i}，于是定理得证．

在上面的证明中只引用了 G 中元的阶数是 p 的幂这一性质．于是假如 G 是有穷群，其中任意元的阶数都是 p 的幂，那末 G 也是循环 p 群的直积，因此 G 也是 p 群．也就是说，一个(有穷)群如果它的任意元的阶数是质数 p 的幂，那末它就是 p 群．

定理 2 p 群 G 能够一意地分解为循环 p 群的直积，也就是

说，假如

$$G=(a_1)\times\cdots\times(a_h)=(b_1)\times\cdots\times(b_k),$$

那末 $h=k$，并且适当选取 (b_1)，…，(b_k) 的顺序，可以使 $(a_i)\cong(b_i)$. 即 a_i 的阶数 p^{r_i} 与 b_i 的阶数 p^{s_i} 相等.

证明 分解的可能性已如上述，下面我们用反证法来证明分解的唯一性.

为了便于叙述，我们假定

$$r_1\geqslant r_2\geqslant\cdots\geqslant r_h,\quad s_1\geqslant s_2\geqslant\cdots\geqslant s_k.$$

假如 $$r_1=s_1,\quad\cdots,\quad r_{i-1}=s_{i-1},\quad r_i<s_i,$$

因为

$$G^{p^{r_i}}=(a_1)^{p^{r_i}}\times\cdots\times(a_h)^{p^{r_i}}=(a_1^{p^{r_i}})\times\cdots\times(a_h^{p^{r_i}}),$$

所以 $G^{p^{r_i}}$ 的元数为

$$p^{r_1-r_i}\cdots p^{r_{i-1}-r_i}=p^{(r_1+\cdots+r_{i-1})-(i-1)r_i}.$$

同样，又因为 $G_p^{p^{r_i}}=(b_1^{p^{r_i}})\times\cdots\times(b_k^{p^{r_i}})$，所以 $G_p^{p^{r_i}}$ 的元数为

$$p^{s_1-r_i}\cdots p^{s_{i-1}-r_i}p^{s_i-r_i}\cdots=p^{(s_1+\cdots+s_{i-1}+s_i)-ir_i+\cdots}.$$

于是

$$r_1+\cdots+r_{i-1}-(i-1)r_i=s_1+\cdots+s_{i-1}+s_i-ir_i+\cdots.$$

因此 $r_i=s_i+\cdots$，即 $r_i\geqslant s_i$，这与上面假设不合. 于是 $r_i=s_i$，因此 $h=k$，所以定理成立.

关于一般有穷群的构造我们有

定理 3 假定群 G 的元数是 n，把 n 分解为质数幂 p_i 的乘积，即 $n=p_1^{r_1}\cdots p_m^{r_m}$，那末 G 能够一意地分解为 $p_i^{r_i}$ 元西洛子群 G_{p_i} 的直积，即

$$G=G_{p_1}\times\cdots\times G_{p_m}.$$

证明 假如 G_i 是 G 中所有适合 $x^{p_i^{r_i}}=e$ 的元 x 的集合，如果 $a^{p_i^{r_i}}=e$，$b^{p_i^{r_i}}=e$，因为 G 是可换群，显然 $(ab)^{p_i^{r_i}}=e$，所以 G_i 是 G 的子群，因此 G_i 的元数是 p_i 的幂.

下面我们根据定义来验证 G 是 G_i 的直积.

首先假设 $q_i=\frac{n}{p_i^{r_i}}$，那末 $q_1, \cdots, q_m$ 的最大公约数是 1，因此有整数 $\lambda_1, \cdots, \lambda_m$ 存在，使

$$\lambda_1 q_1+\cdots+\lambda_m q_m=1$$

成立．于是 G 中任意元 g 能够写成

$$g=g^{\lambda_1 q_1+\cdots+\lambda_m q_m}=g^{\lambda_1 q_1}\cdots g^{\lambda_m q_m}.$$

但
$$(g^{\lambda_i q_i})^{p_i^{r_i}}=(g^{q_i p_i^{r_i}})^{\lambda_i}=(g^n)^{\lambda_i}=e,$$

因此 $g^{\lambda_i q_i}\in G_i$．这就是说，G 中任意元 g 能够表为 G_i 中元的乘积.

再假如 G 的单位元 $e=g_1\cdots g_m$，$g_i\in G_i$，因为 $g_i^{p_i^{r_i}}=e$，所以 $g_j^{q_i}=e$，$i\neq j$，于是

$$g_1^{q_i}\cdots g_i^{q_i}\cdots g_m^{q_i}=e,$$

即
$$g_i^{q_i}=e.$$

但 q_i 与 $p_i^{r_i}$ 互质，于是由 $\mu_i q_i+\nu_i p_i^{r_i}=1$，我们有

$$g_i=(g_i^{q_i})^{\mu_i}(g_i^{p_i^{r_i}})^{\nu_i}=e.$$

因此根据定义，G 是 G_i 的直积.

又比较 G 及 G_i 的元数得知 G_i 的元数是 $p_i^{r_i}$，再 G 中 $p_i^{r_i}$ 元子群显然只有 G_i，因此 $G_i=G_{p_i}$，于是定理成立.

特别，假如 G 是元数 $n=p_1^{r_1}\cdots p_m^{r_m}$ 的循环群，因为循环群的子群仍然是循环群，所以 G 能够分解为 $p_i^{r_i}$ 元循环群 (a_i)，$i=1, \cdots, m$，的直积，即

$$G=(a_1)\times\cdots\times(a_m).$$

由定理 3 及定理 2，我们有

定理 4 有穷群能够一意地分解为循环 p 群的直积.

譬如 12 元可换群是它的 4 元子群与 3 元子群的直积．因为 4 元可换群如果不是循环群，它就是克莱茵 4 元群，也就是两个 2 元

群的直积．所以 12 元可换群有两种类型：一类是循环群，它是 4 元群与 3 元群的直积；另一类是非循环群，它是两个 2 元群与一个 3 元群的直积．

上面讨论的是有穷可换群，现在我们来讨论无穷可换群的构造．但是一般的无穷可换群的构造非常复杂，下面我们只讨论由有穷个元生成的可换群，它是可换群中重要的一类．

要注意的是，假如有穷个生成元的阶数都是有穷，显然由它们生成的可换群是有穷群；就是由它们生成的非可换群，勃恩散特也认为是有穷群．这是 1902 年勃恩散特提出的一个没有证明的定理，是所谓的勃恩散特问题．半个世纪来讨论这问题的虽然大有人在，但只是解决了某些特殊情况，直到 1963 年 П. С. 诺维柯夫提出否定的证明，因此勃恩散特问题得到否定的解答[7]．

假如群 G 是由 n 个元生成，但不能由少于 n 个元生成，那末由 n 个元组成的生成元集，就叫做 G 的**极小生成元集**．一个群如果是由有穷个元生成，那末它就有极小生成元集．

一个群假如除单位元外，任意元的阶都是无穷时，这群我们叫做**纯无穷群**．譬如所有整数对加法形成的群是纯无穷群．一般无穷循环群及无穷循环群的直积也都是纯无穷群．

下面我们先来讨论纯无穷群的构造．

定理 5 由有穷个元生成的纯无穷群能够一意地分解为无穷循环群的直积．

证明 假如 $a_1, \cdots, a_n$ 是群 G 的这样一组极小生成元集，在它们之间满足象下面这种关系：

(3) $$a_1^{\lambda_1}\cdots a_n^{\lambda_n}=e, \quad e \text{ 是 } G \text{ 的单位元},$$

的整数 λ_i 只有完全都是零，也就是它们是与 § 4.4 中线性无关类似，这时我们容易证明 G 中任意元 g 能够一意地表为 $g=a_1^{r_1}\cdots a_n^{r_n}$，于是

$$G=(a_1)\times\cdots\times(a_n),$$

这里(a_i)显然都是无穷循环群. 因此如果我们能够证明 G 的极小生成元集中有象(3)那种线性无关的,那末 G 就是(a_i)的直积. 下面我们用反证法来证明这事实.

假如 G 的极小生成元集中没有象(3)那种线性无关的，显然在这些关系的所有正幂中存在最小的,我们命(3)就是这样的一个关系,其中 λ_1 是最小正幂. 假定

$$\lambda_i=q_i\lambda_1+\mu_i,\quad 0\leqslant\mu_i<\lambda_1,\quad i=2,\ \cdots,\ n,$$

那末 $b=a_1a_2^{q_2}\cdots a_n^{q_n}$, a_2, $\cdots$, a_n 又是 G 的生成元集，它们有关系

$$b^{\lambda_1}a_2^{\mu_2}\cdots a_n^{\mu_n}=e.$$

因为 $0\leqslant\mu_i<\lambda_1$，而 λ_1 是最小正幂，所以 $\mu_2=\cdots=\mu_n=0$. 于是 $b^{\lambda_1}=e$. 但 G 是纯无穷群,所以 $b=e$，因此 a_2, $\cdots$, a_n 就成为 G 的生成元集,这与 a_1, $\cdots$, a_n 是极小生成元集的假设不合,所以 G 的极小生成元集中有象(3)那种线性无关的,因此 G 是(a_i)的直积.

再与 § 4.4 定理 2 类似，假如 G 是(a_1), $\cdots$, (a_n)的直积，那末 G 中任意 $n+1$ 个元都没有象(3)那种线性无关的,因此 G 的直积因子(a_i)的个数 n 是一意的. 又因为无穷循环群都同构，所以 G 能够一意地分解为 n 个无穷循环群的直积. 因此定理成立.

定理 6 由有穷个元生成的群能够一意地分解为有穷群与纯无穷群的直积.

证明 假定 H 是 G 中所有阶数是有穷的元的集合，我们容易得知 H 是 G 的子群. 再 G 的生成元在 $\overline{G}=G/H$ 中的象,显然就是 $\overline{G}$ 的生成元,因此 $\overline{G}$ 也是由有穷个元生成的群.此外,$\overline{G}$ 又是纯无穷群. 这是因为,对于 $\overline{G}$ 中任意元 $\overline{a}\neq\overline{e}$, 这里 $\overline{e}$ 是 $\overline{G}$ 的单位元,如果 $\overline{a}^r=\overline{a^r}=\overline{e}$,那末 $a^r\in H$，因此 a^r 的阶数是有穷，所以 a 的阶数也是有穷，于是 $a\in H$，因此 $\overline{a}=\overline{e}$, 这与上面的假设不合,所以 $\overline{G}$ 中任意元($\neq$单位元)的阶都是无穷，也就是说，$\overline{G}$ 是纯无穷群.

于是由定理 5, $\bar{G}$ 是无穷循环群$(\bar{a}_1)$, …, $(\bar{a}_k)$的直积,即

$$\bar{G}=(\bar{a}_1)\times\cdots\times(\bar{a}_k).$$

命 $K=(a_1)\times\cdots\times(a_k)$, 这里 a_i 是 $\bar{a}_i$ 在 G 中象源, 因为 $\bar{a}_1$, …, $\bar{a}_k$ 的阶都是无穷, 所以 a_1, …, a_k 的阶也都是无穷. 于是 K 是纯无穷群. 下面我们来验证 $G=K\times H$.

首先,对于 G 中任意元 g, 由 $\bar{g}\in\bar{G}$,我们有

$$\bar{g}=\bar{a}_1^{r_1}\cdots\bar{a}_k^{r_k}=\overline{a_1^{r_1}\cdots a_k^{r_k}},$$

因此
$$g=h\cdot a_1^{r_1}\cdots a_k^{r_k},\quad h\in H.$$

即 $g=hk$, $h\in H$, $k\in K$. 再因为 H 中元的阶数都是有穷, 而 K 是纯无穷群, 所以 $H\cap K=E$(G 的单位元群), 因此 G 是 H, K 的直积.

再假如 G 又能分解为有穷群 H' 与纯无穷群 K' 的直积, 即 $G=H'\times K'$. 因为 $K'\cong G/H'$ 是纯无穷群,所以 H' 是 G 中所有阶数是有穷的元形成的子群. 因此 $H'=H$, 于是 $K\cong K'$. 这就是说, G 分解为有穷群与纯无穷群的直积是一意的.

于是定理完全成立.

根据上面三个定理, 我们容易推得下面的**可换群基本定理**[5].

定理 7 由有穷个元生成的群能够一意地分解为循环 p 群与无穷循环群的直积.

这定理的基本内容高斯已早知道,但完备的证明是 1879 年弗罗宾纽斯和施梯克尔贝尔格尔(L. Stickelberger)首先给出的.

上面各定理中的 G 我们没有考虑它的算子集, 也可以说它的算子集是整数环 Z. 假如算子集是体,或者是主理想子环环,上面的定理也都能够同样成立[9].

下面我们来补证 §2.3 中提出而没有给出证明的定理.

假定 G 是 n 元可换群, $n=p_1^{r_1}\cdots p_k^{r_k}$, $m=p_1^{s_1}\cdots p_k^{s_k}$, $s_i\leqslant r_i$, 因为 $G=G_{p_1}\times\cdots\times G_{p_k}$, G_{p_i} 是循环 p 群的直积; 又因为对于循环群, 拉

格朗日定理成立，因此得知 G_{p_i} 有 $p_i^{r_i}$ 元子群，命其一为 H_i，于是

$$H = H_1 \times \cdots \times H_k$$

就是元数为 m 的子群. 这就是说，如果 $m|n$，那末 G 有 m 元子群. 因此当 G 是可换群时，拉格朗日定理的逆是成立的.

再我们用归纳法来证明西洛定理.

假如 $p|c_0$，c_0 是 G 中心 C 的元数. 命 $c_0=p^r s$，于是 C 有元数是 p^r 的 p 西洛子群 H. 因为 H 是 C 的子群，所以它是 G 的正规子群，因此有商群 $\overline{G}=G/H$，这时 $\overline{G}$ 的元数 $p^{a-r}q<n$. 由归纳法假设，$\overline{G}$ 有元数是 p^{a-r} 的 p 西洛子群 $\overline{K}$. 假定 $\overline{K}$ 在 G 的完全象源是 K，那末

$$K \text{ 的元数}=\overline{K} \text{ 的元数}\times H \text{ 的元数}=p^{a-r}\cdot p^r=p^a,$$

因此 K 就是所求的 p 西洛子群.

假如 $p\nmid c_0$，因为 $p|n$，所以在 G 的群方程 $n=c_0+c_1+\cdots+c_r$ (§2.4)中，有某个 c_k 而 $p\nmid c_k$. 假定 a_k 是这共轭类中一元，H 是 G 中所有与 a_k 能够交换的元形成的群，由§2.4，H 的元数为 $\frac{n}{c_k}=p^a\frac{q}{c_k}<n$. 由归纳法假设，$H$ 有元数是 p^a 的 p 西洛子群 K，显然 K 就是所求的 p 西洛子群.

于是西洛定理完全证明成立.

最后我们还来介绍可换群的一个重要性质.

假定 G 是可换群，F' 是可换体 F 的乘群，如果 χ 是 G 射到 F' 的同态，那末 χ 叫做 G 在 F **的群指标**，或者简称为 G 的**群指标**. 两个群指标 χ_1，χ_2，如果对于 G 中任意元 a，有 $\chi_1(a)=\chi_2(a)$，那末 χ_1，χ_2 就相等，即 $\chi_1=\chi_2$. 它们的乘积 $\chi_1\chi_2$，我们规定是

$$\chi_1\chi_2(a)=\chi_1(a)\cdot\chi_2(a),$$

因此 $\chi_1\chi_2$ 又是 G 在 F 的群指标. 我们容易知道，G 在 F 的所有群指标形成可换群 G'，叫做 G 在 F **的群指标群**，或者简单地叫做

G 的群指标群. 这时群指标

$$\chi_0(a)=e, \quad e \text{ 是 } F' \text{ 的单位元},$$

是 G' 的单位元.

下面是有穷可换群与它的群指标群间的一个基本性质.

假定 G 是有穷可换群, $G=(a_1)\times\cdots\times(a_n)$, n_i 是循环群 (a_i) 的元数. 因为 G 中任意元 a 可以写成

$$a=\prod_{i=1}^{n} a_i^{r_i}, \quad 0\leqslant r_i<n_i,$$

所以 $\chi(a)=\prod\limits_{i=1}^{n}\chi(a_i)^{r_i}$. 再因为 $\chi(a_i)$ 是 $x^{n_i}=e$ 的零点, 并且 $x^{n_i}=e$ 在 F 中的所有零点形成一个循环群 (a_i'), 它的元数 m_i 是 n_i 的因数, 即 $m_i|n_i$, 所以 $\chi(a_i)=a_i'^{s_i}$, $0\leqslant s_i<m_i$. 我们命 χ_i 是使 $a=\prod\limits_{i=1}^{n}a_i^{r_i}$ 对应于 $a_i'^{r_i}$ 的群指标, 即 $\chi_i(a)=a_i'^{r_i}$. 也就是说,

$$\chi_i(a_i)=a_i', \quad \chi_i(a_j)=e, \quad i\neq j.$$

因此
$$\chi(a)=\prod_{i=1}^{n}(a_i'^{r_i})^{s_i}=\prod_{i=1}^{n}\chi_i(a)^{s_i},$$

所以
$$\chi=\prod_{i=1}^{n}\chi_i^{s_i}.$$

也就是说, 这时 G' 中任意元 χ 可以写成 χ_i 的乘积.

设 H 是 n 个无穷循环群 (b_i) 的直积, 即 $H=(b_1)\times\cdots\times(b_n)$, 我们命 H 中元 $\prod\limits_{i=1}^{n}b_i^{r_i}$ 与 G 中元 $\prod\limits_{i=1}^{n}a_i^{r_i}$ 对应, 这对应显然是 H 射到 G 上的同态, 因此

$$G\simeq H/K_1,$$

这里 K_1 是 H 中所有形状象 $\prod\limits_{i=1}^{n}b_i^{t_i}$, $t_i\equiv 0(n_i)$, 的元形成的子群. 同样, 我们有

$$G'\simeq H/K_2,$$

这里 K_2 是 H 中所有形状象 $\prod_{i=1}^{n} b_i^{t_i}$, $t_i \equiv 0(m_i)$，的元形成的子群.
因为 $m_i|n_i$，所以 $K_2 \supseteq K_1$. 假定 K 是 H/K 中 K_2/K_1 在 G 的完全象源，由第一同态定理，我们有

$$G/K \cong H/K_1 / K_2/K_1 \cong H/K_2 \cong G'.$$

假如 G 的元数是 d，而 F 含有 d 的本原单位根，因而 F 也含有 n_i 的本原单位根，于是 $x^{n_i}=e$ 在 F 中完全分裂，因此 $m_i=n_i$.
所以 $K_1=K_2$. 显然这时 $K=E$，因此 $G\cong G'$. 于是我们有

定理 8　有穷可换群 G 与它在 F 的群指标群 G' 同态. 假如 G 的元数是 d，而 F 含有 d 的本原单位根，那末 G 与 G' 同构.

习　题　5.5

1. 18 元可换群有几种分解？也就是说，它有几种类型？

2. 有穷可换群成为循环群的必要充分条件是：群的元数为群中所有元素阶数的最小公倍.

3. 任意有穷可换群 G 能够分解为元数是 n_i 的循环群 (a_i) 的直积，即

$$G=(a_1)\times\cdots\times(a_m),$$

并且

$$n_i | n_{i+1}, \quad i=1, 2, \cdots, m-1.$$

4. 假定可换群 $G=\{a_1, \cdots, a_n\}$，试证

$$\begin{aligned}\Sigma\chi(a_i)&=ne, \quad 当\ \chi=\chi_0,\\ &=0, \quad 当\ \chi\neq\chi_0.\end{aligned}$$

§5.6　可迁群，非迁群

这节我们来讨论由变换形成的群，下章我们将要引用它.

我们知道克莱茵四元群

$$B_4=\{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

及

$$B=\{1, (1\,2), (3\,4), (1\,2)(3\,4)\}$$

都是由4个文字1, 2, 3, 4上的排列形成的群，前者含把1变为1, 2, 3, 4的各个排列；但后者则否，它只含把1变为1, 2的排列，不含把1变为3或4的排列．这是变换群的一个基本性质，一般变换群可以根据这性质来分类．

定义 假定G是集合M上变换群的子群，a是M中某元，如果对于M中任意元b，G中就有使$\sigma(a)=b$的变换σ，那末G叫做M的**可迁群**，否则就叫做M的**非迁群**．

于是B是4个文字上的非迁群，B_4是4个文字上的可迁群．n个文字上的对称群S_n及交代群A_n显然都是可迁群．

要注意的是，在上面定义中，元a可以任意选取，不影响群的可迁性．这是因为，假如G是M的可迁群，$\sigma(a)=b$，$\tau(a)=c$，那末

$$\tau\sigma^{-1}(b)=\tau(a)=c,$$

因此对于M中的任意两元b, c，G中含有把b变为c的变换．

可迁群又可象下面那样再分类．

假如G是M的可迁群，如果M能够分为一个以上没有公共元的子集$M_1, M_2, \cdots$，并且M_i的元数不完全都是1，使G中任意变换能够把每个M_i变为一个M_j，那末G就叫做**非原群**，而$M_1, M_2, \cdots$，叫做G的**非原系**．如果M不能这样分，那末G就叫做**本原群**．

譬如对称群S_n是本原群，这是因为，假如它是非原群，命$M_1=\{1, \cdots, k-1, k\}$，那末对换$(k, k+1)$把$M_1$变为$M_2=\{1, \cdots, k-1, k+1\}$，这时$M_1\neq M_2$，而$M_1\cap M_2=\{1, \cdots, k-1\}$，这与非原系的性质不合，所以$S_n$是本原群．同样，交代群$A_n$也是本原群．再$B_4$是非原群，而

$$M_1=\{1, 2\},\ M_2=\{3, 4\};\quad M_1=\{1, 3\},\ M_2=\{2, 4\};$$
$$M_1=\{1, 4\},\ M_2=\{2, 3\}$$

都是它的非原系. 因此我们得知一个非原群的非原系不是唯一的.

假如 G 是非原群, M_1, M_2, …是它的非原系, 那末 G 中含有把 M_i 中元 a_i 变为 M_j 中元 a_j 的变换, 这变换显然就把 M_i 变为 M_j, 所以 M_i 的元数等于 M_j 的元数, 因此非原系 M_1, M_2, …的各个元数都相等. 假如 M 的元数是质数, 那末 G 就是本原群.

下面我们来介绍可迁群的几个基本性质.

假如 G 是 M 的可迁群, 显然 G 中所有不使 M 中元 a 变动的变换形成一个子群 G_a, 陪集 τG_a 中任意变换把 a 变为 $\tau(a)$, 于是 $\tau G_a\tau^{-1}$ 不使 $\tau(a)$ 变动, 因此 $\tau G_a\tau^{-1}\subseteqq G_{\tau(a)}$. 同样, $\tau^{-1}G_{\tau(a)}\tau$ 不使 a 变动, 所以 $\tau^{-1}G_{\tau(a)}\tau\subseteqq G_a$, 这就是说, $G_{\tau(a)}\subseteqq \tau G_a\tau^{-1}$. 因此我们有

$$G_{\tau(a)}=\tau G_a\tau^{-1}.$$

再假如我们把 G_a 的陪集 τG_a 与 $\tau(a)$ 对应, 这对应显然是一对一的. 因为 G 是可迁群, 所以 G 中陪集 τG_a 的个数等于 M 的元数, 也就是说, G 关于 G_a 的指标 $(G:G_a)$ 等于 M 的元数.

此外我们还有

定理 1 假定 G 是集合 M 的可迁群, G_a 是其中不使 M 中元 a 变动的所有变换形成的子群, 那末 G 是非原群的必要充分条件是 G 有适合下面关系的子群 H:

$$G\supset H\supset G_a.$$

证明 假定 G 是非原群, M_1, M_2, …是它的非原系, M_1 的元数大于 1, a 是 M_1 中元, 显然 G 中所有把 M_1 中元仍然变为 M_1 中元, 也就是说不使 M_1 变动的变换形成一个子群, 我们命它为 H. 因为 H 包含 G 中所有不使元 a 变动的变换, 又包含把 a 变为 M_1 中其他元的变换, 所以 $H\supset G_a$. 再因为 G 是可迁群, 所以它包含把 a 变为 M_2 中元的变换, 因此 $G\supset H$. 这就是说,

$G\supset H\supset G_a$. 所以必要条件成立.

反过来，假如 H 是 G 的子群，并且 $G\supset H\supset G_a$，我们把 G 分为若干个 H 的陪集 $\tau_i H$，显然集合

$$M_i=\tau_i H(a)$$

的个数不小于 2，并且每个集合都包含两个以上的元. 因为 G 包含把 a 变为 M 中任意元的变换，所以 M 中任一元必在某个 M_i 中. 再任意两个 M_i, M_j 没有公共元，这是因为，假如

$$\tau_i\sigma_i(a)=\tau_j\sigma_j(a),\quad \sigma_i,\ \sigma_j\in H,$$

那末 $\sigma_j^{-1}\tau_j^{-1}\tau_i\sigma_i(a)=a$，因此

$$\sigma_j^{-1}\tau_j^{-1}\tau_i\sigma_i\in G_a\subset H,$$

于是 $\tau_i\in\tau_j H$，这与假设不合. 因此 M 能够分为这样的 M_i 类. 又假如 ρ 是 G 中任意元，因为

$$\rho M_i=\rho\tau_i H(a)=\tau_j H(a)=M_j,$$

所以 ρ 把 M_i 变为 M_j，因此 G 是非原群，所以充分条件成立. 于是定理得证.

对于体，也有所谓本原的与非原的之分. 假如 K 是 F 的有穷次代数体，如果 K 中不属于 F 的元都是关于 F 的本原元，那末 K 叫做 F 的**本原体**；否则就叫做**非原体**.

最后我们介绍非迁群的基本性质.

假如 G 是集合 M 的非迁群，我们可以把 M 这样来分类，先在 M 中任取一元，把 M 中 G 的各变换对于这元的所有象作为一子集，再在 M 中任取不属于这子集的一元，把这元的所有象又作为一子集，这样继续下去，我们可以把 M 分为若干个这样没有公共元的子集. 显然对于任意子集中某一元，G 中有把它变为这集中任一元的变换，并且 G 中任意变换把这任意子集中元仍然变为这集中元. 也就是说，对于这些子集来说，G 都是可迁的. 这些子集我们又叫它做 G 的**可迁系**.

譬如$\{1, 2\}$, $\{3, 4\}$就是非迁群B的可迁系.

要注意的是，虽然可迁群的非原系中各个子集的元数是相等的，但是非迁群的可迁系中各个子集的元数却不一定相等，譬如

$$\{1, (1\,2\,3), (1\,3\,2), (4\,5)(1\,2\,5)(4\,5), (1\,3\,2)(4\,5)\}$$

是集合$\{1, 2, 3, 4, 5\}$的非迁群，它的可迁系是$\{1, 2, 3\}$, $\{4,5\}$.

定理2 假定可迁群G的正规子群H是非迁群，那末H的可迁系中各个子集的元数相等.

证明 假如G是关于$\{1, 2, \cdots, m\}$的可迁群，$\{1, 2, \cdots, k\}$, $k<m$, 是H的可迁系中一子集，我们命i是不属这子集的任意数. 因为G是可迁，所以它含有把1变为i的变换. 假定$\sigma(1)=i$, 那末$\sigma(1), \sigma(2), \cdots, \sigma(k)$又是$\sigma H\sigma^{-1}=H$的可迁系中一子集. 这是因为，$H$中含有把1变为$\{1, 2, \cdots, k\}$中任意元的变换，因此$\sigma H\sigma^{-1}$中含有把$\sigma(1)$变为$\{\sigma(1), \sigma(2), \cdots, \sigma(k)\}$中任意元的变换. 假如$\sigma H\sigma^{-1}$中含有把$\sigma(1)$变为$\sigma(k+1)$的变换，那末$H$中就有把1变为$k+1$的变换，这与假设不合. 因此$\sigma(1), \sigma(2), \cdots, \sigma(k)$是$H$的可迁系中一子集. 因为$i$是任意数，所以$H$的可迁系中任一子集都是由$k$个数组成，这就是说，$H$的可迁系中各个子集的元数相等，因此定理成立.

在上面的证明中，假如m是质数，因为$k|m$, 那末$k=1$, 于是我们得知，对于元数是质数的集合的可迁群，它的正规子群除单位元群外，都是可迁群.

习 题 5.6

1. 假如G是M的可迁群，G的元数是n, M的元数是m, 试证$m|n$.

2. 假定G是$M=\{1, 2, \cdots, m\}$的可迁群，G_i是G中所有不使i变动的变换形成的子群，试证$G_1, G_2, \cdots, G_m$中任意两个群共轭. 假如M中对于G_k中任意变换都不动的数字的个数是m_k, 那末G_k的正规化群的元数是

$g_k m_k$，这里 a_k 是 G_k 的元数.

3. 假定 $G=\{g_1, g_2, \cdots, g_k\}$ 是 $\{a_1, a_2, \cdots, a_m\}$ 的可迁群，$H=\{h_1, h_2, \cdots, h_l\}$ 是 $\{b_1, b_2, \cdots, b_n\}$ 的可迁群，试证 kl 个排列

$$g_i h_j, \quad i=1, 2, \cdots, k; \quad j=1, 2, \cdots, l,$$

形成 $\{a_1, \cdots, a_m, b_1, \cdots, b_n\}$ 的非迁群，并且 $\{a_1, a_2, \cdots, a_m\}$，$\{b_1, b_2, \cdots, b_n\}$ 是它的可迁系.

4. 试证对称群 S_6 的子群

$$H=\{(1), (1\,4\,5)(2\,3\,6), (1\,5\,4)(2\,6\,3), (1\,2)(3\,5)(4\,6), (1\,3)(2\,4)(5\,6), (1\,6)(2\,5)(3\,4)\}$$

是 $M=\{1, 2, 3, 4, 5, 6\}$ 的非原群，并求出它的所有非原系.

参 考 文 献

[1] W. E. Barnes, Introduction to abstract algebra (1963), 89～92.

[2] Bender, Helmut, A group theoretic proof of Burnside's $p^a q^b$-theorem, Math. Z., 126 (1972), 327～338.

[3] (1) Hua, Loo-Keng (华罗庚), On the multiplicative groups of a field, 科学记录，第三卷第一期 (1950), 1～6.

(2) W. R. Scott, On the multiplicative group of a division ring, Proc. Amer. Math. Soc., 8 (1957), 303～305.

[4] W. Feit and J. G. Thompson, Solvability of groups of odd order, Pacific Jour. of Math., Vol. 13, No. 3 (1963).

[5] (1) I. Kaplansky, Infinite abelian groups, The University of Michigan Press. Ann Arbor, 1962.

(2) L. Fuchs, Abelian Groups, Pergamon Press, New York, 1967.

(3) R. Hirshon, On Cancellation in groups, Amer. Math. Monthly, 76 (1969) 1037～1039.

(4) ——, Cancellation of Groups with maximal condition, Proc. Amer. Math. Soc., 24 (1970), 401～403.

(5) ——, The Cancellation of an infinite cyclic group in direct products, Arch. Math. (Basel), 26 (1975), 134～138.

[6] N. 贾柯勃逊著抽象代数学（黄缘芳译），卷 1 第五章，143～144.

[7] A. П. 吉兹曼，周期群的伯恩赛德问题，数学通报，9 (1963), 33.

[8] E. Schenkman, The basis theorem for finitely generated abelian groups, Amer. Math. Monthly, 67 (1960), 770～771.

[9] N. Jacobson, The Theory of Rings (1943), 43～44.

第六章

伽罗瓦理论

这章是介绍有穷次可离正规体的伽罗瓦理论，它在代数及代数数论上都占重要地位．前三节是介绍基本概念及基本性质，后四节主要是讨论多项式用代数解出的问题，是伽罗瓦理论的一个重要应用．这问题是借伽罗瓦理论获得解决的，伽罗瓦理论之来也正是由这问题所引起．很多关于体的问题可以变为体的自同构形成的群的问题来讨论，容易得到解决．这是伽罗瓦理论的基本思想，其重要也就在此．

这章讨论的体都是可换体．

§6.1 伽罗瓦群

我们知道，假定K是可换体F的n次可离体．根据§4.8定理1，我们可以把K写成$K=F(\alpha)$．如果$f(x)$是$F[x]$中α适合的n次既约多项式，L(F的扩张体)是$f(x)$的分裂体，由§4.7定理3，得知在L中，K关于F的同值有n个互异的，并且不论L如何扩大，在同一体中，这样互异的同值不能多于n个．假如$f(x)$在L中的零点是$\alpha_1(=\alpha)$, α_2, $\cdots$, α_n，那末在L中，K关于F的同值是把$f(x)$的零点α仍然变为$f(x)$的零点α_k，因此把$F(\alpha)$中元$\sum\limits_{i=1}^{n} a_i\alpha^i$变为$\sum\limits_{i=1}^{n} a_i\alpha_k^i$，所以这时的同值是把$F(\alpha)$变为它的共轭体

$F(\alpha_k)$，这同值我们用 σ_k 表示，即 $\sigma_k(\alpha)=\alpha_k$.

假如 $K=F(\alpha)$ 又是 F 的正规体，那末 $F(\alpha)=F(\alpha_k)$，所以 K 关于 F 的同值是 K 的自同构．它不使 F 中任意元变动．显然，K 的这样自同构的逆以及任意两个这样自同构的积仍然是这样的自同构．因此所有这样不使 F 中任意元变动的 K 的自同构形成一个群，这群叫做 K 关于 F 的**伽罗瓦群**，或者叫做 K 关于 F 的**群**，我们用 G 来表示．这就是说，K 关于 F 的伽罗瓦群是所有不使 F 中任意元变动的 K 的自同构形成的群．§4.6 中所以叫 K 做 F 的伽罗瓦体，其原因就是 G 叫做伽罗瓦群．

由 §4.7 定理 5，我们得知 G 的元数等于 K 关于 F 的次数 $(K:F)$．于是 K 关于 F 的伽罗瓦群 $G=\{\sigma_1, \cdots, \sigma_n\}$.

上面我们介绍 K 关于 F 的同值是先把 K 写成 F 的单扩张，因此引用了 K 的本原元，但这引用，只是为了方便，并不是非如此不可．假定 K 是由 F 陆续添加 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 形成的扩张体，即 $K=F(\alpha_1, \alpha_2, \cdots, \alpha_n)$，那末在 K 的适当扩张体 L 中，K 关于 F 的同值可以这样来求得．先求出 $F(\alpha_1)$ 关于 F 的同值，这些同值都把 α_1 变成它的共轭元，再将这些同值延长成为 $F(\alpha_1, \alpha_2)$ 的同构，就得到在 L 中 $F(\alpha_1, \alpha_2)$ 关于 F 的所有同值．这样继续做下去，最后将 $F(\alpha_1, \alpha_2, \cdots, \alpha_{n-1})$ 关于 F 的所有同值延长就得到在 L 中 K 关于 F 的所有同值了．

我们知道 G 中任意元不使 F 中任意元变动，它的逆也成立．这就是

定理 1 假定 G 是 K 关于 F 的伽罗瓦群，那末 K 中对于 G 的任意元不变动的元都在 F 中．

证明 因为 K 中任意元 α 适合的 $F[x]$ 中既约多项式的次数等于 α 关于 F 互异的共轭元的个数．如果这个数等于 1，那末 α 就是 F 中元了．假定 α' 是 α 在 K 中关于 F 的任意共轭元，因为

$F(\alpha)$，$F(\alpha')$关于F同值，由§4.6定理3，我们可以把它延长成为K的自同构．因此G中有把α变为α'的元．现在G中所有元都不使α变动，所以$\alpha'=\alpha$，这就是说α的共轭元只有它自身，即α的共轭元的个数等于1，因此定理得证．

于是K中元在F中的必要充分条件是：它的伽罗瓦群G中任意元不使它变动，这是伽罗瓦群一个最基本的性质．再由上面的证明，我们又得知，假如α，β是K中关于F的共轭元，那末G中有把α变为β的元．

可换体F的有穷次正规体，当它关于F的伽罗瓦群是阿贝耳群时，就叫做F的阿贝耳体，是循环群时，就叫做F的循环体．

下面我们给出几个伽罗瓦群的例．

假定Q是有理数体，$K=Q(\omega,\sqrt[3]{2})$，$\omega=\dfrac{1}{2}(-1+i\sqrt{3})$，因为$\sqrt[3]{2}$，$\omega$分别是$Q$中既约多项式

$$x^3-2=(x-\sqrt[3]{2})(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2}),$$

$$x^2+x+1=(x-\omega)(x-\omega^2)$$

的零点，而K关于Q的伽罗瓦群G中元把它们的零点仍然变为它们的零点，所以$\sqrt[3]{2}$的象只能有3个，ω的象只能有2个．于是合并它们就得到下面6个不使Q中元变动的K的自同构：

	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$
ω	ω	ω	ω	ω^2	ω^2	ω^2

因为$(K:Q)=6$，所以这6个自同构就是G的全部元，即

$$G=\{1,\ \sigma,\ \sigma^2,\ \tau,\ \sigma\tau,\ \sigma^2\tau\}.$$

再由计算容易得知

$$\sigma^3=1,\quad \tau^2=1,\quad \tau\sigma=\sigma^2\tau,\quad \tau\sigma^2=\sigma\tau,$$

显然 G 与对称群 S_3 同构，即 $G\cong S_3$．这就是说，K 关于 Q 的伽罗瓦群是 S_3．

又假定 $K=GF(p^n)$，F 是它的质体．对于 K 中任意元 α，我们命 α^p 与它对应，即 $\alpha\to\alpha^p$．因为由 §4.9，K 中任意元 $\alpha=\alpha^{p^n}$，所以 K 中任意元可以写成 γ^p，$\gamma\in K$．又对于 K 中任意两元 α，β，我们有

$$\alpha^p-\beta^p=(\alpha-\beta)^p,$$

如果 $\alpha^p=\beta^p$，那末 $\alpha=\beta$．于是 $\alpha\to\alpha^p$ 是 K 射到自己上的可逆映射．再因为

$$(\alpha+\beta)^p=\alpha^p+\beta^p,\quad (\alpha\beta)^p=\alpha^p\beta^p,$$

所以这映射又是 K 的自同构．当 $\alpha\in F$ 时，$\alpha^p=\alpha$，因此这同构不使 F 中任意元变动，所以它是伽罗瓦群 G 中元，我们用记号 σ 表示，即 $\sigma(\alpha)=\alpha^p$．于是 σ，σ^2，…，$\sigma^n=1$ 都是 G 中元．由 §4.9 我们知道，K 中有阶数为 p^n-1 的元，因此这 n 个自同构互异，但 $(K:F)=n$，所以 G 的元数是 n，于是 $G=\{\sigma,\ \sigma^2,\ \cdots,\ \sigma^n=1\}$，即 G 是 n 元循环群，这就是说，有穷体是它的质体的循环体．

再假定 $K=F(\xi)$，ξ 是 n 次本原单位根．我们知道，ξ^{n_k} 是 n 次本原单位根的必要充分条件是 n，n_k 互质，即 $(n,\ n_k)=1$．假如 $n_1,\cdots,n_{\varphi(n)}$ 是模 n 的既约系，σ_i 是 K 关于 F 的伽罗瓦群 G 中任意元，因为它把本原单位根仍然变为本原单位根，所以 $\sigma_i(\xi)=\xi^{n_i}$，因此

$$\sigma_i\sigma_j(\xi)=\sigma_i(\xi^{n_j})=(\sigma_i(\xi))^{n_j}=(\xi^{n_i})^{n_j}=\xi^{n_in_j}=\xi^{n_k},$$

式中 $n_in_j\equiv n_k\ (n)$．因为 $(n_i,\ n)=1$，$(n_j,\ n)=1$，所以 $(n_in_j,\ n)=1$．假如命 n_i 与 σ_i 对应，那末这对应就是 G 的同构，因此 K 的伽罗瓦群 G 可以看成是由 n_1，…，$n_{\varphi(n)}$ 对于模 n 形成的乘群，所以 G 是可换群[1]．这就是说，K 是 F 的阿贝耳体．假如 n 是质数，a 是 n 的本原根，那末 1，a，a^2，…，a^{n-2} 是模 n 的既约系，显然这系对

于模 n 成为 $n-1$ 元循环群，因此 G 是 $n-1$ 元循环群，所以这时 K 就是 F 的循环体.

此外我们还有

定理 2 假定体 F 含有 n 次本原单位根，$K=F(\alpha)$，这里 α 是纯多项式 $f(x)=x^n-a$, $a\in F$, 的零点，也就是说，α 是 F 中某元的 n 次根，那末 K 是 F 的循环体.

证明 假定 ξ 是 F 中 n 次本原单位根. 因为 $\alpha, \xi\alpha, \cdots, \xi^{n-1}\alpha$ 是 K 中 $f(x)$ 的零点. 如果 σ 是 K 关于 F 的伽罗瓦群 G 中元，因为 σ 把 $f(x)$ 的零点仍然变为 $f(x)$ 的零点，所以 $\sigma(\alpha)=\xi^k\alpha$. 我们命 σ 与 ξ^k 对应，即 $\sigma\to\xi^k$，显然这对应是 G 射到由 n 次单位根形成的群内的同构. 由 § 4.9 定理 5, n 次单位根形成的群是循环群，因此它的子群也是循环群. 于是 G 是循环群，所以 K 是 F 的循环体，因此定理成立.

特别，当 $f(x)=x^n-a$ 是既约时，K 关于 F 的次数是 n，因此 K 关于 F 的伽罗瓦群 G 与 n 次单位根形成的循环群同构. 这就是说 G 是 n 元循环群.

上面讨论了 K 关于 F 的伽罗瓦群，下面我们介绍多项式 $f(x)$ 的伽罗瓦群.

假如 $f(x)$ 是 F 的 n 次可离多项式，$\alpha_1, \cdots, \alpha_n$ 是它在同一分裂体中的零点，那末 $K=F(\alpha_1, \cdots, \alpha_n)$ 是 F 的有穷次可离正规体，K 关于 F 的伽罗瓦群 G 又叫做 **$f(x)$ 的伽罗瓦群**. 这时如果 $(K:F)=m$, $G=\{\sigma_0=1, \sigma_1, \cdots, \sigma_{m-1}\}$，显然 $\sigma_i(\alpha_1), \cdots, \sigma_i(\alpha_n)$ 都是 $f(x)$ 的零点. 又因为 σ_i 是 K 关于 F 的同值映射，由于 $\alpha_1, \cdots, \alpha_n$ 互异，所以 $\sigma_i(\alpha_1), \cdots, \sigma_i(\alpha_n)$ 也互异，因此 $\sigma_i(\alpha_1), \cdots, \sigma_i(\alpha_n)$ 是 $\alpha_1, \cdots, \alpha_n$ 的一个排列. 于是对于 σ_i，我们有排列

$$s_i=\begin{pmatrix}\alpha_1 & \cdots & \alpha_n\\ \sigma_i(\alpha_1) & \cdots & \sigma_i(\alpha_n)\end{pmatrix}.$$

假如 $s_i=s_j$，那末 $\sigma_i(\alpha_1)=\sigma_j(\alpha_1)$，…，$\sigma_i(\alpha_n)=\sigma_j(\alpha_n)$. 因为 K 中任意元 α 能够用系数是 F 中元的 α_1，…，α_n 的多项式表出，所以 $\sigma_i(\alpha)=\sigma_j(\alpha)$. 这与 $\sigma_i\neq\sigma_j$ 的假设不合，于是 m 个排列 s_0，s_1，…，s_{m-1} 互异. 再因为

$$s_is_j=\begin{pmatrix}\alpha_1 & \cdots & \alpha_n\\ \sigma_i\sigma_j(\alpha_1) & \cdots & \sigma_i\sigma_j(\alpha_n)\end{pmatrix},$$

因此，如果我们命 σ_i 与 s_i 对应，即 $\sigma_i\to s_i$，那末这对应就是 G 射到 $\{s_0, s_1, \cdots, s_{m-1}\}$ 上的同构，所以 G 与 α_1，…，α_n 上对称群 S_n 的子群同构，也就是说，n 次可离多项式的伽罗瓦群是对称群 S_n 的子群.

同前面类似，一个可离多项式当它的伽罗瓦群是阿贝耳群时，叫做**阿贝耳式**，是循环群时，叫做**循环式**.

譬如 Q 是有理数体，$f(x)=x^3-3x-1$，根据 §4.6 习题 6，我们容易验证 $f(x)$ 是 Q 的正规式，如果 K 是它的分裂体，那末 $(K:Q)=3$，因此 $f(x)$ 的伽罗瓦群 G 是 3 元循环群，但 S_3 中 3 元子群只有 A_3，所以 $G=A_3$. 同样，我们也不难证明 $f(x)=x^3-9x+2$ 是 Q 的正规式，因此它的分裂体关于 Q 的次数是 $3\cdot2=6$，于是 $f(x)$ 的伽罗瓦群 G 是 6 元群，所以 $G=S_3$.

下面是关于可离多项式的伽罗瓦群的一个常用定理.

定理 3 假定 $f(x)$ 是 F 的可离多项式，那末它的伽罗瓦群 G 是可迁群的必要充分条件为 $f(x)$ 是既约式.

证明 假如 $f(x)$ 是既约式，α_1，…，α_n 是它的零点，因为 $F(\alpha_1)\cong F(\alpha_i)$，由 §4.6 定理 3，这同构延长就成为 G 中元，这就是说 G 中有把 α_1 变为任意 α_i 的元，因此 G 是 $\{\alpha_1, \cdots, \alpha_n\}$ 的可迁群.

假如 $f(x)$ 是可约式，$f_1(x)$，$f_2(x)$ 是 $f(x)$ 的两个既约因式，α_1 是 $f_1(x)$ 的零点，α_2 是 $f_2(x)$ 的零点，因为 G 中元把 $f_1(x)$ 的零

点仍然变为 $f_1(x)$ 的零点，所以 G 中没有把 α_1 变为 α_2 的元，因此 G 是 $\{\alpha_1, \cdots, \alpha_n\}$ 的非迁群．

于是定理得证．

譬如 $f(x)=x^4-5x^2+6$ 是关于有理数体 Q 的多项式，因为 $x^4-5x^2+6=(x^2-2)(x^2-3)$，所以其分裂体 $K=Q(\sqrt{2}, \sqrt{3})$．又因为 $f(x)$ 的伽罗瓦群 G 中元把 $\sqrt{2}$ 变为 $\pm\sqrt{2}$，把 $\sqrt{3}$ 变为 $\pm\sqrt{3}$，于是我们得 $G=\{1, \sigma, \tau, \rho\}$，这里

	1	σ	τ	ρ
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$

假如 $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ 分别用 1, 2, 3, 4 来表示，那末

$$1=(1),\ \sigma=(1\,2),\ \tau=(3\,4),\ \rho=(1\,2)(3\,4),$$

显然 G 是非迁群．

习　题　6.1

1．试证 3 次既约多项式的伽罗瓦群是对称群或是交代群．

2．试证 $F[x]$ 中多项式 $f(x)$ 的伽罗瓦群全由偶排列形成的必要充分条件是 $f(x)$ 的判别式的平方根在 F 中．

3．假设 $K=Q(\sqrt{2}, i)$，Q 是有理数体，试求 K 关于 Q 的伽罗瓦群及它的群表．

4．试证 $K=F(\alpha)$，α 是 n 次本原单位根，的伽罗瓦群是可换群．

5．试求下列各多项式关于有理数体的伽罗瓦群：

$$x^3-2,\quad x^3+2x+1,\quad x^4-10x^2+1.$$

6．试证 x^4-5x^2+6 与 x^4-10x^2+1 的分裂体都是 $K=Q(\sqrt{2}, \sqrt{3})$，但前者的伽罗瓦群是非迁群而后者的则是可迁群．

7．假定体 F 含有质数 p 次本原单位根，试证 x^p-a，$a\in F$，在 $F[x]$ 中或是既约，或是完全分裂为一次因式的乘积．

8．假定体 F 不含质数 p 次本原单位根，试证 x^p-a，$a\in F$，在 $F[x]$ 中

或是既约,或是

$$x^p-a=x^p-\alpha^p=(x-\alpha)(x^{p-1}+\alpha x^{p-2}+\cdots+\alpha^{p-1}),$$

这里 $a=\alpha^p$, $\alpha\in F$.

§6.2 伽罗瓦理论的基本定理

这节讨论 K, F 的中间体与 K 关于 F 的伽罗瓦群 G 的子群间的关系,它是伽罗瓦理论的基础.

假如 G_1 是 G 的子群, 那末 K 中所有对于 G_1 中任意元不变动的元形成 K 的子体,这是因为,如果

$$\sigma(\alpha_i)=\alpha_i,\quad \sigma(\alpha_j)=\alpha_j,\quad \sigma\in G_1,\quad \alpha_i,\alpha_j\in K,$$

那就有
$$\sigma(\alpha_i-\alpha_j)=\alpha_i-\alpha_j,\quad \sigma(\alpha_i\alpha_j^{-1})=\alpha_i\alpha_j^{-1}.$$

这子体我们叫做 G_1 **所属的体**, 用 $K(G_1)$ 来表示. 因此 F 是 G 所属的体, K 是单位元群 E 所属的体,即

$$F=K(G),\quad K=K(E).$$

同样,假如 K_1 是 K, F 的中间体,那末 G 中所有不使 K_1 中任意元变动的元形成 G 的子群,这是因为,如果

$$\sigma_i(\alpha)=\alpha,\quad \sigma_j(\alpha)=\alpha,\quad \alpha\in K_1,\quad \sigma_i,\sigma_j\in G,$$

那就有
$$\sigma_i\sigma_j(\alpha)=\alpha.$$

这子群,我们叫做 K_1 **所属的群**, 用 $G(K_1)$ 来表示. 因此 E 是 K 所属的群, G 是 F 所属的群,即

$$E=G(K),\quad G=G(F).$$

由上面的等式,我们得知

$$K(G(F))=F,\quad G(K(E))=E.$$

把 F 换成 K,把 E 换成 G,上面等式也同样成立. 假如把 G_1 与它所属的体 $K(G_1)$对应, 又把 K_1 与它所属的群 $G(K_1)$对应, 那末根据上面等式, F 与 G 一一对应, E 与 K 也一一对应. 但对于任

意 G_1, K_1, 根据定义, 我们有

$$K(G(K_1))\supseteq K_1,\quad G(K(G_1))\supseteq G_1,$$

如果上面不等式都是等式, 那末 K_1 与 $G(K_1)$ 一一对应, G_1 与 $K(G_1)$ 一一对应. 下面的定理就是解答这问题, 它是**伽罗瓦理论的基本定理**.

定理 1　假如 K 是 F 的有穷次可离正规体, G 是 K 关于 F 的伽罗瓦群, 那末

1° K, F 的中间体 K_1 是 $G(K_1)$ 所属的体, 即

$$K(G(K_1))=K_1;$$

2° G 的子群 G_1 是 $K(G_1)$ 所属的群, 即

$$G(K(G_1))=G_1;$$

3° $G(K_1)$ 的元数等于 $(K:K_1)$, G 关于 $G(K_1)$ 的指标等于 $(K_1:F)$.

这定理的含义我们可以用下面的图式来表示:

$$\begin{array}{ccccc}
\multicolumn{5}{c}{\overbrace{\underbrace{G\ \supseteq\ G_1}_{k}\ \underbrace{\supseteq\ E}_{h}}^{n=kh}}\\
\updownarrow & & \updownarrow & & \updownarrow\\
F & \subseteq & K_1 & \subseteq & K
\end{array}$$

这里 G_1 是 K_1 所属的群, K_1 是 G_1 所属的体.

$$n=\begin{cases}(G:E)=G\ \text{的元数},\\ (K:F)=K\ \text{关于}\ F\ \text{的次数},\end{cases}$$

$$k=\begin{cases}(G:G_1)=G\ \text{关于}\ G_1\ \text{的指标},\\ (K_1:F)=K_1\ \text{关于}\ F\ \text{的次数},\end{cases}$$

$$h=\begin{cases}(G_1:E)=G_1\ \text{的元数},\\ (K:K_1)=K\ \text{关于}\ K_1\ \text{的次数}.\end{cases}$$

证明　首先, 由 §4.6 定理 7 我们得知 K 是 K_1 的正规体. 因此由定义容易得知, $G(K_1)$ 是 K 关于 K_1 的伽罗瓦群, 再由 §6.1

定理 1，K 中对于 $G(K_1)$ 中任意元不变动的元都在 K_1 中，也就是说，$K(G(K_1))\subseteq K_1$，所以

$$K(G(K_1))=K_1,$$

因此 1° 成立．

其次，假如 $G_1=\{\sigma_1,\cdots,\sigma_h\}$，因为 $G(K(G_1))\supseteq G_1$，如果我们能够证明 $G(K(G_1))$ 的元数不大于 h，那末 $G(K(G_1))=G_1$，2° 就告成立．因为 $G(K(G_1))$ 是 K 关于 $K(G_1)$ 的伽罗瓦群，所以我们只要证明 $(K:K(G_1))\leqslant h$ 就行了．现在假设 $K=F(\alpha)$，因为多项式

$$(x-\sigma_1(\alpha))(x-\sigma_2(\alpha))\cdots(x-\sigma_h(\alpha))$$

的系数是 $\sigma_1(\alpha),\cdots,\sigma_h(\alpha)$ 的初等对称多项式，所以它对于任意 σ_i 都不变动，因此它们是 $K(G_1)$ 中的元．再 α 是这多项式的零点，所以 α 关于 $K(G_1)$ 的次数不大于 h，但 $K=K(G_1)(\alpha)$，于是 $(K:K(G_1))\leqslant h$，因此 2° 成立．

最后，因为 $G(K_1)$ 是 K 关于 K_1 的伽罗瓦群，所以 $G(K_1)$ 的元数等于 $(K:K_1)$．再假如 G 的元数是 n，$G(K_1)$ 的元数是 h，$G(K_1)$ 在 G 的指标是 j，那末我们就有 $n=hj$，但

$$(K:F)=n,\ (K:K_1)=h,\ (K:F)=(K:K_1)(K_1:F),$$

所以 $(K_1:F)=j$，因此 3° 成立．

于是定理得证．

上面的定理建立了 K，F 的中间体与伽罗瓦群 G 的子群间一一对应的关系，这是伽罗瓦理论中最基本的一个性质，它已经在多方面得到了推广．

1928 年克努尔把上定理推广到次数是无穷的代数扩张体，1940 年贾柯勃逊推广到一般体，1945 年又推广到不是可离又不是正规体的可换体．1951 年中山正(1912～1964)已经推广到满足极小条件的环了[2]．

假定 $K=F(\alpha)$ 是 F 的可离单扩张体，那末 K, F 的中间体只有有穷个. 这是因为，假如 L 是含 K 的 F 有穷次可离正规体，由于 L 关于 F 的伽罗瓦群是有穷群，所以它的子群只有有穷个. 于是由上面的主要定理得知，L, F 的中间体也只有有穷个，因此 K, F 的中间体只有有穷个. 反过来，假如 K 是 F 的可离体，如果 K, F 的中间体只有有穷个，那末 K 关于 F 是有穷次，因此 K 是 F 的单扩张体.

一般，假如 K 是 F 的可换扩张体，那末 K, F 的中间体只有有穷个是 K 有关于 F 的本原元的必要充分条件. 1942 年阿丁(E. Artin, 1898～1962)有一个简单证明[3]，读者可以取原书参考.

上面是讨论 $K(G_1)$ 与 $G(K_1)$ 的关系，现在我们要问，假如 K_1 已知，$G(K_1)$ 如何去找？假如 G_1 已知，$K(G_1)$ 又如何去找？

假定 $K_1=F(\beta_1, \cdots, \beta_m)$，因为 $K=F(\alpha)$，所以 β_i 是 α 的多项式. 假定 G 中元 σ 把 α 变为 α_k，如果我们在表示 β_i 的 α 的多项式中把 α 换成 α_k，仍然是这个多项式，那末 σ 就不使 β_i 变动. G 中不使 $\beta_1, \cdots, \beta_m$ 变动的元也不使 K_1 中任意元变动，因此所有这些元形成的子群就是 $G(K_1)$.

假定 $G_1=\{\sigma_1, \cdots, \sigma_m\}$，由前面得知多项式

$$(x-\sigma_1(\alpha))(x-\sigma_2(\alpha))\cdots(x-\sigma_m(\alpha))$$

的系数都在 $K(G_1)$ 中，因此把这些系数添加于 F 得到的体 $K'\subseteq K(G_1)$，并且 $(K:K')\leqslant m$，由 § 4.4 定理 4，$(K(G_1):K')=1$，因此 $K'=K(G_1)$. 这就是说，把 $\sigma_1(\alpha), \cdots, \sigma_m(\alpha)$ 的初等对称多项式添加于 F 得到的体就是所求的 $K(G_1)$.

例如在 § 6.1 中，$K=Q(\omega, \sqrt[3]{2})$ 关于 Q 的伽罗瓦群

$$G=\{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

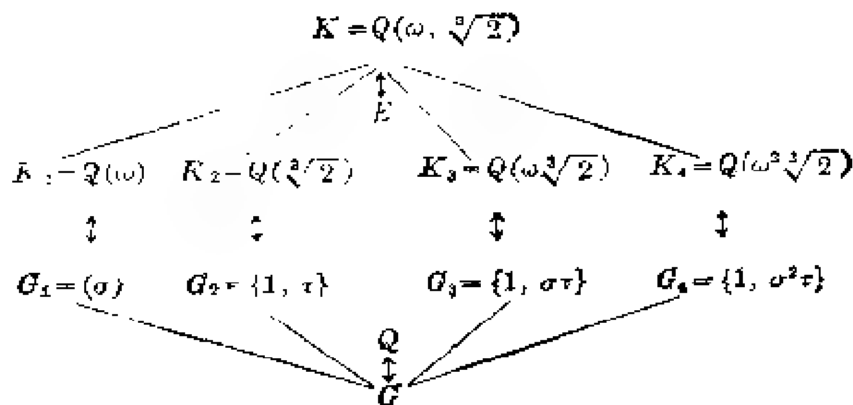
显然它有一个 3 元子群 $G_1=\{1, \sigma, \sigma^2\}$，三个 2 元子群

$$G_2=\{1, \tau\}, \quad G_3=\{1, \sigma\tau\}, \quad G_4=\{1, \sigma^2\tau\}.$$

由计算我们容易得知，与它们对应的子体分别为

$$K_1=Q(\omega),\quad K_2=Q(\sqrt[3]{2}),$$
$$K_3=Q(\omega\sqrt[3]{2}),\quad K_4=Q(\omega^2\sqrt[3]{2}).$$

它们之间的对应关系用图式表示如下：



假如 K_1, K_2 是 K, F 的中间体，G 是 K 关于 F 的伽罗瓦群，G_1, G_2 分别是 K 关于 K_1, K_2 的伽罗瓦群，即分别是 K_1, K_2 所属的群，它们之间还有下面一些重要性质.

定理 2 假如 $K_1\supset K_2$，那末 $G_1\subset G_2$；反过来，假如 $G_1\subset G_2$，那末 $K_1\supset K_2$.

证明 假如 $K_1\supset K_2$，因为 K 的自同构如果不使 K_1 中任意元变动，显然也不使 K_2 中任意元变动，所以 $G_1\subseteq G_2$. 又因为 G_2 是 K 关于 K_2 的伽罗瓦群，所以对于在 K_1 中而不在 K_2 中的任意元，G_2 中必有一元使它变动，因此 $G_1\subset G_2$.

再假如 $G_1\subset G_2$，显然 $K_1\supseteq K_2$. 如果 $K_1=K_2$，那末 $G_1=G_2$，这与假设不合；因此 $K_1\supset K_2$. 所以定理得证.

我们知道，假如 G 中有元把 K_1 变成 K_2，那末 K_1, K_2 关于 F 同值. 因此 K_1, K_2 关于 F 共轭(§4.3). 反过来，假定 K_1, K_2 关于 F 共轭，也就是说 K_1, K_2 关于 F 同值，由 §4.6 定理 3，这同值可以延长成为 K 的自同构，所以 G 中有元把 K_1 变为 K_2.

于是 K_1, K_2 关于 F 是共轭体的必要充分条件是 G 中有元把 K_1 变为 K_2, 因此 α_1, α_2 是共轭元的必要充分条件是 G 中有元把 α_1 变成 α_2. 再由 §4.6 定理 6, 我们又得知, 中间体 K_1 是 F 的正规体的必要充分条件是 G 中任意元不使它自身变动.

定理 3　假如 K_1, K_2 关于 F 共轭, 那末 G_1, G_2 共轭; 反过来, 假如 G_1, G_2 共轭, 那末 K_1, K_2 关于 F 共轭.

证明　假如 K_1, K_2 关于 F 共轭, 我们命 $K_1=F(\alpha)$, 那末 $K_2=F(\sigma(\alpha))$, $\sigma\in G$. 显然 $\sigma G_1\sigma^{-1}$ 中任意元不使 $\sigma(\alpha)$ 变动, 因此也不使 K_2 中任意元变动, 所以 $\sigma G_1\sigma^{-1}\subseteqq G_2$. 同样, 我们可以把 K_1 写成 $K_1=F(\sigma^{-1}(\sigma(\alpha)))$, 因此 $\sigma^{-1}G_2\sigma\subseteqq G_1$. 于是 $G_2\subseteqq\sigma G_1\sigma^{-1}$, 所以 $G_2=\sigma G_1\sigma^{-1}$, 即 G_1, G_2 共轭.

再假如 G_1, G_2 共轭, 命 $G_2=\sigma G_1\sigma^{-1}$, $\sigma\in G$, 根据上面的证明, 我们知道 $F(\sigma(\alpha))$ 所属的群是 $\sigma G_1\sigma^{-1}$, 也就是说是 G_2, 因此 $K_2=F(\sigma(\alpha))$, 于是 σ 把 K_1 变成 K_2, 即 K_1, K_2 关于 F 共轭. 所以定理成立.

假定 K_1 与它的共轭体一致, 那末 G_1 就与它的共轭群一致, 因此我们得到下面中间体是正规体的必要充分条件.

定理 4　K_1 是 F 的正规体的必要充分条件为 G_1 是 G 的正规子群.

此外, 在 K 与 G 之间还有很多类似的性质, 譬如 K 是可解体时, G 就是可解群; 反过来, G 是可解群时, K 就是可解体.

再假如我们已经知道 K 关于 F 的伽罗瓦群, 那末我们不仅可以知道 K 关于任意中间体 K_1 的伽罗瓦群, 由下面定理, 我们还可以知道 K_1 关于 F 的伽罗瓦群.

定理 5　假如 K_1 是 F 的正规体, 那末 K_1 关于 F 的伽罗瓦群 $G'\cong G/G_1$.

证明　因为 K_1 是 F 的正规体, 所以 G 中任意元 σ 诱导出

G' 中一元 σ'. 由 §4.6 定理 3,我们又得知,G' 中任意元可以延长成为 G 中元,因此假如命 σ' 与 σ 对应, 即 $\sigma\to\sigma'$, 这对应显然就是 G 射到 G' 上的同态. 但这同态核是 G_1, 由 §2.5 定理 5 即得 $G'\cong G/G_1$,因此定理成立。

习 题 6.2

1. 假设 G 是 K 关于 F 的伽罗瓦群,G_1, G_2 是 G 的子群,试证 (G_1, G_2) 所属的体是 $K(G_1)\cap K(G_2)$, $G_1\cap G_2$ 所属的体是 $F(K(G_1), K(G_2))$.

2. 假如 G 是 K 关于 F 的伽罗瓦群, K_1, K_2 是 K, F 的中间体, 试证 $F(K_1, K_2)$所属的群是 $G(K_1)\cap G(K_2)$, $K_1\cap K_2$ 所属的群是

$$(G(K_1),\ G(K_2)).$$

3. 假如 K 是 F 的扩张体, $F(\alpha)$是 F 的正规体, 试证 $K(\alpha)$关于 K 的伽罗瓦群与 $F(\alpha)$关于 F 的伽罗瓦群一致的必要充分条件是

$$F(\alpha)\cap K=F.$$

4. 假如 K 是 F 的阿贝耳体, 试证 K, F 的任意中间体是 F 的正规体, 并且又是 F 的阿贝耳体.

5. 假如 K 是 F 的正规体, $K\supsetneqq L\supsetneqq F$, F' 是 K 中包含 L 的最小 F 的正规体, 试证 F' 所属的群是 L 所属的群与它的共轭群的交集.

6. 假如 Q 是有理数体, $K=Q(i, \sqrt[4]{2})$, 求 K 关于 Q 的伽罗瓦群, 并求它的子群所属的 K 的子体.

7. 假定 K 是 F 的有穷次不可离正规体, 它的特征数是 p, L 是 K 中 F 的最大可离体, $(L:F)=n_0$, 那末 K 的所有不使 F 中任意元变动的自同构形成的群 G, 叫做 K 关于 F 的伽罗瓦群, 试证:

1) G 的元数等于 n_0, 即 G 的元数等于 K 关于 F 的缩减次数.

2) G 是 L 关于 F 的伽罗瓦群.

3) 假定 K_1 是 K, F 的中间体, 那末 $G(K_1)=G(L_1)$, 这里 L_1 是 K_1 中 F 的最大可离体.

4) 假定 G_1 是 G 的子群, 那末 $K_1=K(G)$中任意元的 p 次根仍在 K_1中.

5) $G(K(G_1))=G_1$.

6) 假定 K_1 中任意元的 p 次根仍在 K_1 中, 那末 $K(G(K_1))=K_1$.

这就是说, 定理 1 能够这样推广到不可离体。

§6.3 正 规 底

有穷次可离正规体的伽罗瓦理论包含四个主要定理，上节的定理 1 及定理 4 是其中两个，这节我们介绍其他两个．因为正规底存在的证明较麻烦，所以这节大部分篇幅是介绍这证明．

假定 G 是由可换体 K 的 n 个自同构形成的群，F 是 K 中所有对于 G 中任意元不变动的元的集合，显然 F 是 K 的子体．现在我们要问，G 是否就是 K 关于 F 的伽罗瓦群？假如我们能够证明 $(K:F)\leqslant n$，那末由 §4.7 定理 4，$(K:F)=n$，因此由 §4.7 定理 5，K 是 F 的可离体，于是 K 是 F 的 n 次可离正规体，所以 G 是 K 关于 F 的伽罗瓦群．

定理 1 假定 $G=\{\sigma_1, \cdots, \sigma_n\}$ 是由可换体 K 的自同构形成的群，F 是 K 中所有对于任意 σ_i 不变动的元形成的子群，那末 $(K:F)=n$．

证明 假定 $\alpha_1, \cdots, \alpha_{n+1}$ 是 K 中任意 $n+1$ 个非零的元，由 §4.4 定理 2，我们容易得知，$n+1$ 个向量

$$\delta_i=(\sigma_1(\alpha_i), \cdots, \sigma_n(\alpha_i)), \quad i=1, 2, \cdots, n+1,$$

关于 K 线性相关．假定 $\delta_1, \cdots, \delta_r$ 是其中元数最大的线性无关元组，因为 $r\leqslant n$，那末

$$\delta_{r+1}=a_1\delta_1+\cdots+a_r\delta_r, \quad a_i\in K,$$

因此 $\quad \sigma_k(\alpha_{r+1})=a_1\sigma_k(\alpha_1)+\cdots+a_r\sigma_k(\alpha_r), \quad k=1, 2, \cdots, n.$

但 $\sigma_1\sigma_k, \cdots, \sigma_n\sigma_k$ 是 G 的全部元，命 $\sigma_j\sigma_k=\sigma_l$，我们就有

$$\sigma_l(\alpha_{r+1})=\sigma_j(a_1)\sigma_l(\alpha_1)+\cdots+\sigma_j(a_r)\sigma_l(\alpha_r),$$
$$l=1, 2, \cdots, n.$$

把这式中的 l 改写成 k，同上式比较就得到

$$\{a_1-\sigma_j(a_1)\}\sigma_k(\alpha_1)+\cdots+\{a_r-\sigma_j(a_r)\}\sigma_k(\alpha_r)=0,$$

$$k=1,\ 2,\ \cdots,\ n.$$

因为 $\delta_1, \cdots, \delta_r$ 关于 K 线性无关，所以 $\sigma_j(a_i)=a_i$，这就是说，a_i 对于任意 σ_j 不变，因此 $a_i\in F$. 假定 σ_1 是恒等映射，即 $\sigma_1=1$，那末

$$\alpha_{r+1}=a_1\alpha_1+\cdots+a_r\alpha_r,$$

于是 $\alpha_1, \cdots, \alpha_r, \alpha_{r+1}$ 关于 F 线性相关，这就是说，K 中任意 $n+1$ 个元关于 F 线性相关，因此 $(K:F)\leqslant n$，所以定理成立.

于是我们得知，假如 G 是由可换体 K 的自同构形成的有穷群，F 是 K 中所有对 G 中任意元不变动的元形成的子体，那末 K 是 F 的有穷次可离正规体. 反过来，假如 K 是 F 的有穷次可离正规体，那末所有不使 F 中任意元变动的 K 的自同构形成的群就是 K 关于 F 的伽罗瓦群 G. 显然它是有穷群. 因此我们得伽罗瓦理论中第三个主要定理.

定理 2 假定 F 是可换体 K 的子体，那末由 K 的所有不使 F 中任意元变动的自同构形成的群 G 是有穷群的必要充分条件为：K 是 F 的有穷次可离正规体.

下面正规底存在定理是伽罗瓦理论中第四个主要定理. 这定理在 1932 年由多伊林(M. Deuring, 1907～)首先证明，自后也还有其他证明，但直到 1950 年以前，所有这些证明都要引用表现理论. 虽然 1942 年阿丁有一个不引用表现理论的证明，但它只限于 F 不是有穷体的情形，因此不是一个完备的证明. 这里我们介绍的证明是 1950 年伽塞斯 (J. W. S. Gasseis) 及华尔 (G. E. Wall) 提出的，它是一个不需要表现理论的初等证明[4].

定理 3 假定 K 是 F 的 n 次可离正规体，$G=\{\sigma_1, \cdots, \sigma_n\}$ 是它的伽罗瓦群，那末 K 中有元 α，使

$$\sigma_1(\alpha),\ \sigma_2(\alpha),\ \cdots,\ \sigma_n(\alpha)$$

成为 K 关于 F 的底，这底我们叫做 K 关于 F 的**正规底**.

证明 我们知道，齐次线方程组有非零解的必要充分条件是：

它的系数行列式等于零，因此我们容易得知，K 中元 $\alpha_1, \cdots, \alpha_n$ 如果适合

$$\begin{vmatrix} \sigma_1^{-1}(\alpha_1) & \cdots & \sigma_1^{-1}(\alpha_n) \\ \cdots & \cdots & \cdots \\ \sigma_n^{-1}(\alpha_1) & \cdots & \sigma_n^{-1}(\alpha_n) \end{vmatrix} = |\sigma_i^{-1}(\alpha_j)| \neq 0,$$

那末它们就关于 F 线性无关，因此也就是 K 关于 F 的底．于是 K 中元 α 如果适合 $|\sigma_i^{-1}(\sigma_j(\alpha))| \neq 0$，那末 $\sigma_1(\alpha), \cdots, \sigma_n(\alpha)$ 就是 K 关于 F 的正规底．

现在分两段来证明 K 中有这样的元 α 存在．

1．当 F 不是有穷体时．

假定 σ_1 是 G 的单位元，并且规定当 $\sigma_i^{-1}\sigma_j = \sigma_k$ 时，$(i, j) = k$，于是

$$f(x_1, \cdots, x_n) = \begin{vmatrix} x_{(1,1)} & \cdots & x_{(1,n)} \\ \cdots & \cdots & \cdots \\ x_{(n,1)} & \cdots & x_{(n,n)} \end{vmatrix}$$

是 $K[x_1, \cdots, x_n]$ 中多项式．取 $x_1 = 1$, $x_i = 0$, $i \neq 1$，因为 $(i, i) = 1$, $(i, j) \neq 1$, $i \neq j$，显然

$$f(1, 0, \cdots, 0) = \begin{vmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{vmatrix} = 1 \neq 0,$$

因此 $f(x_1, \cdots, x_n) \neq 0$，即 $f(x_1, \cdots, x_n)$ 不恒等于零，但

$$f(\sigma_1(\alpha), \cdots, \sigma_n(\alpha)) = \begin{vmatrix} \sigma_1^{-1}\sigma_1(\alpha) & \cdots & \sigma_1^{-1}\sigma_n(\alpha) \\ \cdots & \cdots & \cdots \\ \sigma_n^{-1}\sigma_1(\alpha) & \cdots & \sigma_n^{-1}\sigma_n(\alpha) \end{vmatrix}$$
$$= |\sigma_i^{-1}\sigma_j(\alpha)|.$$

假如在 K 中我们能够找到元 α 使 $f(\sigma_1(\alpha), \cdots, \sigma_n(\alpha)) \neq 0$，那末 $|\sigma_i^{-1}\sigma_j(\alpha)| \neq 0$，因此 $\sigma_1(\alpha), \cdots, \sigma_n(\alpha)$ 就是 K 关于 F 的正规底．

下面我们在 K 中来找满足 $f(\sigma_1(\alpha), \cdots, \sigma_n(\alpha)) \neq 0$ 的元 α．

假定 $\alpha_1, \cdots, \alpha_n$ 是 K 关于 F 的底，那末 $|\sigma_i(\alpha_j)|\neq 0$，于是命

$$x_i=\sigma_i(\alpha_1)y_1+\cdots+\sigma_i(\alpha_n)y_n,\quad i=1, 2, \cdots, n,$$

我们有

$$f(x_1, \cdots, x_n)=f\left(\sum_{i=1}^n\sigma_1(\alpha_i)y_i, \cdots, \sum_{i=1}^n\sigma_n(\alpha_i)y_i\right)$$

$$=g(y_1, \cdots, y_n),$$

因为 $f(x_1, \cdots, x_n)\neq 0$，由 §3.10 习题 4，$K$ 中有元

$$\beta_i=\sigma_i(\alpha_1)y_1+\cdots+\sigma_i(\alpha_n)y_n,\quad i=1, 2, \cdots, n,$$

使 $f(\beta_1, \cdots, \beta_n)\neq 0$，因为 $|\sigma_i(\alpha_j)|\neq 0$，所以上面线性方程组在 K 中有唯一组解 $\gamma_1, \cdots, \gamma_n$，因此 $g(\gamma_1, \cdots, \gamma_n)=f(\beta_1, \cdots, \beta_n)\neq 0$。这就是说，$g(y_1, \cdots, y_n)\neq 0$。再因为 $g(y_1, \cdots, y_n)$ 的系数是 K 中元，又由 §3.10 习题 4，F 中有元 $a_1, \cdots, a_n$ 使 $g(a_1, \cdots, a_n)\neq 0$，命

$$\alpha=\alpha_1a_1+\cdots+\alpha_na_n,$$

那末

$$f(\sigma_1(\alpha), \cdots, \sigma_n(\alpha))=f\left(\sum_{i=1}^n\sigma_1(\alpha_i)a_i, \cdots, \sum_{i=1}^n\sigma_n(\alpha_i)a_i\right)$$

$$=g(a_1, \cdots, a_n)\neq 0,$$

因此这时定理成立.

2. 当 F 是有穷体时.

由 §6.2，我们得知 K 是 F 的循环体，假如 $\alpha_1, \cdots, \alpha_n$ 是 K 关于 F 的底，σ 是 K 关于 F 的伽罗瓦群 G 的生成元，即 $G=(\sigma)$，命

$$\alpha=\sum_{i=1}^n a_i\alpha_i,\quad a_i\in F,$$

那末

$$|\sigma^{-i}(\sigma^j(\alpha))|=|\sigma^{-i+j}(\alpha)|=\left|\sum_{k=1}^n a_k\sigma^{-i+j}(\alpha_k)\right|=|\beta_{-i+j}|.$$

这里
$$\beta_i=\sum_{j=1}^n a_j\sigma^i(\alpha_j),\quad \beta_{i\pm n}=\beta_i.$$

假如在 K 中能找出 α，就是说，在 F 中能找出 a_i 使多项式

$$g(x)=\sum_{i=0}^{n-1}\beta_i x^i$$

与 $f(x)=x^n-1$ 互质，那末 $\sigma_1(x), \cdots, \sigma_n(x)$ 就是正规底，这是因为在 $K[x]$ 中有满足

$$s(x)g(x)+t(x)(x^n-1)=1$$

的多项式 $s(x)$, $t(x)$. 再我们取 n 级矩阵

$$A=\begin{pmatrix} 0 & 1 & \ddots & 0 \\ \ddots & 0 & 1 & \ddots \\ 0 & \ddots & \ddots & 1 \\ 1 & 0 & \ddots & 0 \end{pmatrix},$$

由计算我们容易得知

$$A^2=\begin{pmatrix} 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 1 \\ \vdots & & & \ddots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & 1 & \cdots & \cdots & 0 \end{pmatrix},$$

$$A^m=\begin{pmatrix} \overbrace{0 \quad \ddots}^{m+1} & 1 & \ddots & 0 \\ \ddots & \ddots & \ddots & 1 \\ 1 & \ddots & \ddots & \ddots \\ \underbrace{0 \quad \ddots \quad 1}_{m} & \ddots & & 0 \end{pmatrix}, \quad 0<m<n, \ A^n=1.$$

把这 A 代上式的 x，得矩阵等式 $s(A)g(A)=1$，于是 $|s(A)|\,|g(A)|=1$，但

$$g(A)=\beta_0A^0+\beta_1A^1+\cdots+\beta_{n-1}A^{n-1}$$

$$=\begin{pmatrix} \beta_0 & \ddots & 0 \\ \ddots & \ddots & \ddots \\ 0 & \ddots & \beta_0 \end{pmatrix}+\begin{pmatrix} 0 & \beta_1 & \ddots & 0 \\ \ddots & \ddots & \ddots & \beta_1 \\ \beta_1 & & \ddots & 0 \end{pmatrix}+\cdots+\begin{pmatrix} 0 & \ddots & \beta_{n-1} \\ \beta_{n-1} & \ddots & \ddots \\ 0 & \ddots\ \beta_{n-1} & 0 \end{pmatrix}=(\beta_{-i+j}),$$

因此$|\beta_{-i+j}|\neq 0$,所以$\sigma_1(\alpha)$, …, $\sigma_n(\alpha)$是K关于F的正规底.

下面我们来求使$g(x)$与$f(x)=x^n-1$互质的a_i.

假定$L\supseteq K$是$f(x)=x^n-1$的分裂体，b_1, …, b_m $(m\leqslant n)$是$f(x)$在L中互异零点. 因为$(L:F)\geqslant n$, 在L中我们可以适当挑选b_{m+1}, …, b_n, 使b_1, …, b_m, b_{m+1}, …, b_n互异. 如果$g(b_i)\neq 0$ $(i=1, 2, \cdots, n)$，那末$g(x)$与$f(x)$在K的扩张体中没有公共零点,因此$g(x)$就是与$f(x)$互质的了.

我们把$g(b_j)$写成

$$g(b_j)=\sum_{i=1}^{n} a_i\left(\sum_{k=0}^{n-1}\sigma^k(\alpha_i)b_j^k\right)=\sum_{i=1}^{n} a_i q_{ij},$$

这里

$$q_{ij}=\sum_{k=0}^{n-1}\sigma^k(\alpha_i)b_j^k.$$

因为α_1, …, α_n是K关于F的底，所以$|\sigma^k(\alpha_i)|\neq 0$, 又因为$b_1$, …, b_n互异,所以

$$|b_j^k|=\prod_{n\geqslant s>t\geqslant 1}(b_s-b_t)\neq 0,$$

因此

$$|q_{ij}|=|\sigma^k(\alpha_i)|\,|b_j^k|\neq 0.$$

假定β_1, …, β_r是L关于F的底,

$$q_{ij}=\sum_{k=1}^{r} b_{ij}^{(k)}\beta_k,\quad b_{ij}^{(k)}\in F,$$

因为

$$|q_{ij}|=\sum_{\lambda_1\cdots\lambda_n=1}^{r}\beta_{\lambda_1}\cdots\beta_{\lambda_n}|b_{ij}^{(k)}|,$$

所以其中有某个$|b_{ij}^{(l)}|\neq 0$. 于是在F中有满足

$$\sum_{i=1}^{n} a_i b_{ij}^{(l)}=1,\quad j=1, 2, \cdots, n,$$

的元a_i. 如果这时

$$g(b_j)=\sum_{i=1}^{n} a_i q_{ij}=\sum_{k=1}^{r}\left(\sum_{i=1}^{n} a_i b_{ij}^{(k)}\right)\beta_k=0,$$

因为β_1, …, β_r关于F线性无关，那末$\sum_{i=1}^{n} a_i b_{ij}^{(l)}=0$, 这与上面矛

盾，所以 $g(b_i)\neq 0$. 这就是说，象上面这样挑选的 a_i 可以使 $g(x)$ 与 $f(x)$ 互质，因此定理得证.

§6.4　多项式能够用根号解出的条件

在复数体中，1, 2, 3, 4 次多项式的零点都可以由复数用有理运算及根号来表出，这是我们早已知道的. 现在我们要问，5 次及 5 次以上多项式的零点是否也能如此？此后两节就一般情形来讨论这问题，这节我们先讨论它的必要充分条件.

我们先证明 §6.1 定理 2 的逆定理以备引用.

定理 1　假定体 F 含有 n 次本原单位根，K 是 F 的 n 次循环体，那末 $K=F(\gamma)$，这里 γ 是纯多项式 x^n-a, $a\in F$ 的零点.

证明　假定 $K=F(\alpha)$，σ 是 K 关于 F 的伽罗瓦群 G 的生成元，ξ 是 F 中的 n 次本原单位根，

$$\vartheta_i=\alpha+\xi^i\sigma(\alpha)+\cdots+\xi^{(n-1)i}\sigma^{n-1}(\alpha),\quad i=0,1,\cdots,n-1.$$

显然 $\vartheta_i\in K$. 因为 $\sigma^n(\alpha)=\alpha$，所以我们有

$$\begin{aligned}\sigma(\vartheta_i)&=\sigma(\alpha)+\xi^i\sigma^2(\alpha)+\cdots+\xi^{(n-2)i}\sigma^{n-1}(\alpha)+\xi^{(n-1)i}\alpha\\&=\xi^{-i}\{\alpha+\xi^i\sigma(\alpha)+\cdots+\xi^{(n-1)i}\sigma^{n-1}(\alpha)\}=\xi^{-i}\vartheta_i,\end{aligned}$$

于是 $\sigma(\vartheta_i^n)=\vartheta_i^n$，因此 ϑ_i^n 对 G 中任意元不变，所以 $\vartheta_i^n=a_i\in F$，这就是说，ϑ_i 是 $F[x]$ 中纯多项式 x^n-a_i 的零点.

再因为

$$(1-\xi^k)(1+\xi^k+\xi^{2k}+\cdots+\xi^{(n-1)k})=1-(\xi^k)^n=0,$$

并且当 $k=1, 2, \cdots, n-1$ 时，$1-\xi^k\neq 0$，所以

$$\sum_{i=0}^{n-1}\xi^{ki}=0\quad(1\leqslant k\leqslant n-1).$$

于是

$$\sum_{i=0}^{n-1}\vartheta_i=n\alpha+\sum_{i=1}^{n-1}\xi^i\sigma(\alpha)+\cdots+\sum_{i=0}^{n-1}\xi^{(n-1)i}\sigma^{n-1}(\alpha)=n\alpha.$$

因此，$\vartheta_0, \vartheta_1, \cdots, \vartheta_{n-1}$ 不都在 F 中．假如 $\vartheta_k \in F$，因为 $x^n - a_k$ 在 F 中是既约的(§6.1 习题7)，所以 $K = F(\vartheta_k)$，这就是说，K 关于 F 的本原元 ϑ_k 是纯多项式的零点，所以定理成立．

要注意的是，假如 F 的特征数是 p，定理中 n 就不能被 p 整除．这是因为如果不如此，首先 F 的 n 次本原单位根不存在．再因为 $x^n - a$ 是 x^p 的多项式，所以它的零点都是重零点，把它添加于 F 得到的体不是可离体．

现在我们来讨论多项式能够用根号解出的条件，首先为了便于叙述，我们引用下面的定义．

因为 $x^n - a$ 的零点我们常常叫做 a 的 n 次根，写成 $\sqrt[n]{a}$，所以上面的 $F(\alpha)$ 又叫做 F 的根号扩张体．又因为 $n = n_1 n_2$ 时，$x^n - a = (x^{n_1})^{n_2} - a$ 的零点可以看成 $x^{n_1} - \sqrt[n_2]{a}$ 的零点．因此

$$\sqrt[n]{a} = \sqrt[n_1]{\sqrt[n_2]{a}}.$$

于是我们有如下定义：

假设 K 是体 F 的扩张体，如果它们之间有中间体

$$F = F_0 \subset F_1 \subset \cdots \subset F_n = K, \quad F_i = F_{i-1}(\alpha_i),$$

这里 $\alpha_i^{p_i} \in F_{i-1}$，$p_i$ 是质数，那末 K 就叫做 F 的**根号扩张体**．$F[x]$ 中多项式，如果它的分裂体是 F 的根号扩张体的子体，就叫做**能够用根号解出**．

于是循环式能够用根号解出．

为了方便，下面我们假定所需要的质数 p_i 次本原单位根都已包含在基础体 F 中，因此 F 的特征数异于 p_i．

再要注意的是，F 的有穷次根号扩张体 $K = F_m$ 不一定是 F 的正规扩张体，但可以再用根号来扩张使它成为 F 的正规扩张体．这是因为，首先，由于 p_1 次本原单位根都在 F 中，所以 $f_1(x) = x^{p_1} - a_1$，$a_1 \in F$ 的所有零点也都在 F_1 中，也就是说 F_1 是 $f_1(x)$ 的分裂体，因此 F_1 是 F 的正规体．如果 $K = F_1$，也就是说

$m=1$，那末 K 就是 F 的正规体．如果 $K\supset F_1$，也就是说 $m\neq 1$，因为 $F_2=F_1(\alpha_2)$，α_2 是 $x^{p_1}-a_2$，$a_2\in F_1$，的零点，命 σ 是 F_1 关于 F 的伽罗瓦群中任意元，那末

$$f_2(x)=\prod_{\sigma}(x^{p_2}-\sigma(a_2))$$

是 $F[x]$ 中多项式．我们把 $f_2(x)$ 的零点都添加于 F_1 就得到 F_2 的扩张体 L_2，因为 F 包含 p_2 次本原单位根，所以 L_2 是 $F[x]$ 中多项式 $f_1(x)f_2(x)$ 的分裂体，因此是 F 的正规体．如果 $K\subseteq L_2$，即 $m=2$，那末 L_2 就是所求的正规体；如果 K 不是 L_2 的子体，即 $m>2$，我们用同样方法继续添加根号，经过有穷回后，终可得到包含 K 的 F 的正规体 L，所以 K 再用根号扩张可以成为 F 的正规体．

下面是多项式能够用根号解出的必要条件，这里的多项式我们假定是没有重零点的．

定理 2　假定 $F[x]$ 中多项式 $f(x)$ 能够用根号解出，并且 F 的特征数不能整除根号的次数，那末它的伽罗瓦群是可解群．

证明　假设 K 是 $f(x)$ 的分裂体，因为 $f(x)$ 能够用根号解出，所以 K 是 F 的根号扩张体的子体．由上面的讨论，我们得知 K 有这样的扩张体 L 存在，它是 F 的正规体，并且在它与 F 之间有中间体

$$F=F_0\subset F_1\subset\cdots\subset F_m=L,$$

这里 $F_i=F_{i-1}(\alpha_i)$，$\alpha_i^{p_i}\in F_{i-1}$．因为 F 含有 p_i 次本原单位根，所以 F_i 是 F_{i-1} 的正规体．假设 G 是 L 关于 F 的伽罗瓦群，G_i 是 F_i 所属的子群，于是我们有

$$G=G_0\supset G_1\supset\cdots\supset G_m=E.$$

因为 F_i 是 F_{i-1} 的正规体，所以 G_i 是 G_{i-1} 的正规子群，且 G_{i-1}/G_i 是 F_i 关于 F_{i-1} 的伽罗瓦群，因此 G_{i-1}/G_i 的元数是 p_i．于是它是循环群，也就是可换群，所以 G 是可解群．但 K 是 F 的正规

体，因此 $G/G(K)$ 是 K 关于 F 的伽罗瓦群，也就是 $f(x)$ 的伽罗瓦群．因为 G 是可解群，由 §5.3 定理 7，$G/G(K)$ 也是可解群，所以 $f(x)$ 的伽罗瓦群是可解群，因此定理成立．

在上定理中，如果 F 的特征数能够整除根号的次数，那末 $f(x)$ 的分裂体 K 是 F 的不可离体，这时它的伽罗瓦群就不在我们讨论的范围内．

下面我们来证明根号解出的充分条件．

定理 3　假定 $F[x]$ 中多项式 $f(x)$ 的伽罗瓦群 G 是可解群，并且 F 的特征数不能整除 G 的元数，那末 $f(x)$ 能够用根号解出．

证明　我们知道有穷群有合成群列．一个群如果有合成群列，那末它的任意正规群列可以加细使成为合成群列．又假如 $A\supset B\supset C$，其中 B，C 都是 A 的正规子群，如果 A/C 是可换群，由 §5.2 第一同构定理，

$$A/B\cong A/C\Big/B/C,$$

所以 A/B 是可换群．再因为可换群只有元数是 1 或是质数时才是单群，于是我们容易得知，这时 G 有合成群列

$$G=G_0\supset G_1\supset\cdots\supset G_m=E,$$

这里商群 G_{i-1}/G_i 是元数为质数 p_i 的循环群．因此 F 的特征数异于 p_i，命 F_i 是 K 中属于 G_i 的子体，于是我们有

$$F=F_0\subset F_1\subset\cdots\subset F_m=K.$$

因为 G_{i-1} 是 G_i 的正规子群，所以 F_i 是 F_{i-1} 的正规体，再因为 F_i 关于 F_{i-1} 的伽罗瓦群 G_{i-1}/G_i 是 p_i 次循环群，所以 F_i 是 F_{i-1} 的 p_i 次循环体．但我们已假定 F 中含有 p_i 次本原单位根，由定理 1，$F_i=F_{i-1}(\alpha_i)$，这里 $\alpha_i^{p_i}\in F_{i-1}$，所以 K 是 F 的根号扩张体，因此 $f(x)$ 能够用根号解出，所以定理获证．

我们要注意的是，在上面定理中，如果没有 F 的特征数不能

整除 G 的元数这条件，那末定理1就不能引用，因此定理就不能够成立．也就是说，多项式 $f(x)$ 的伽罗瓦群虽是可解群，如果 F 的特征数与 G 的元数不互质，那末 $f(x)$ 不一定能够用根号解出．譬如，假定 F 是特征数为2的质体，u, v 是关于 F 的未定元，$K=F(u, v)$ 是 F 的超越体，那末2次多项式

$$f(x)=x^2+ux+v$$

显然是可离的，因此 $f(x)$ 的分裂体是 K 的2次可离体，于是 $f(x)$ 的伽罗瓦群的元数是2，所以它是可解群．但是添加奇数次纯多项式的零点于 K 得到的扩张体关于 K 是奇数次，添加偶数次纯多项式的零点于 K 得到的扩张体是 K 的不可离体，因此 $f(x)$ 的分裂体不可能是 K 的根号扩张体的子体，这就是说，$f(x)$ 不能够用根号解出．

再要注意的是，在上面讨论中，我们假定 F 含所需要的质数 p_i 次本原单位根只是为了方便，如果没有这假定，上面的定理2及定理3仍然是同样成立的，其理由如下：

假如 $f(x)$ 的分裂体 K 是 F 的根号扩张体 L 的子体，我们把 $(L:F)$ 次本原单位根添加于 K 得到体 K'，添加于 F 得到体 F'，这时 K' 是 F 的正规体，因此 K' 也是 F' 的正规体．命 K' 关于 F 及 F' 的伽罗瓦群分别是 G 及 G'，显然 G' 是 G 的正规子群，因为 K' 是 F' 的根号扩张体的子体，由定理3，G' 是可解群，再因为 G/G' 是 F' 关于 F 的伽罗瓦群，由§6.1的习题4，它是可换群，因此 G 是可解群(§5.3习题2)．但 $f(x)$ 的伽罗瓦群是 $G/G(K)$，而它又是可解群 G 的商群，所以 $f(x)$ 的伽罗瓦群是可解群．

再假如 $f(x)$ 的分裂体是 $K=F(\alpha_1, \cdots, \alpha_n)$，它的伽罗瓦群 G 是可解群，元数是 m．因为 F 的特征数不能整除 m，所以 F 的 m 次本原单位根存在．假定把它添加于 F 得到的体是 F'，那末 $K'=F'(\alpha_1, \cdots, \alpha_n)$ 是把 $f(x)$ 看成 $F'[x]$ 中多项式时的分裂体，因

为 K' 关于 F' 的伽罗瓦群 G' 中任意元把 α_i 变为 α_j，也就是说，它决定 $\alpha_1, \cdots, \alpha_n$ 的一个排列，并且它不使 F' 中元变动，因此也不使 F 中任意元变动，所以它又决定 G 中一元。再因为 G' 中两个不同的元所决定 $\alpha_1, \cdots, \alpha_n$ 的排列不同，因此它所决定的 G 中元也不同．于是 G' 与 G 的子群同构，所以 G' 可以看成 G 的子群．因为 G 是可解群，所以 G' 也是可解群．因为 G' 的元数是 G 的元数的因数，所以 F' 的特征数不能整除 G' 的元数．由定理 3，K 是 F' 的根号扩张体的子体，因此也是 F 的根号扩张体的子体，所以 K 是 F 的根号扩张体的子体．

§6.5　n 次一般多项式的解

假定 $F(u_1, \cdots, u_n)$ 是可换体 F 的超越扩张体，u_i 是 $F(u_1, \cdots, u_{i-1}, u_{i+1}, \cdots, u_n)$ 的超越元，也就是说，$u_1, \cdots, u_n$ 是 F 的未定元，那末 n 次多项式

$$f(x)=x^n-u_1x^{n-1}+u_2x^{n-2}-\cdots+(-1)^nu_n$$

就叫做 F 的 n 次一般多项式，或简称 n 次**一般多项式**．

假如 $v_1, \cdots, v_n$ 是 $f(x)$ 在它的分裂体 K 中的零点，那末

$$u_1=v_1+\cdots+v_n,\quad u_2=v_1v_2+\cdots+v_{n-1}v_n,\quad \cdots,$$

$$u_n=v_1v_2\cdots v_n,$$

显然 $F(v_1, \cdots, v_n)$ 是 $F(u_1, \cdots, u_n)$ 的扩张体，因此 $K=F(v_1, \cdots, v_n)$．

下面是著名的**阿贝耳定理**．

定理 1　n 次一般多项式 $f(x)$ 的伽罗瓦群是 n 个文字上的对称群 S_n．

证明　我们先来证明零点是未定元的多项式，它的伽罗瓦群是对称群．

假如 $x_1, \cdots, x_n$ 是未定元.

$$\alpha_1 = x_1 + x_2 + \cdots + x_n,$$
$$\alpha_2 = x_1x_2 + \cdots + x_{n-1}x_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\alpha_n = x_1x_2\cdots x_n,$$

那末
$$h(x) = (x-x_1)(x-x_2)\cdots(x-x_n)$$
$$= x^n - \alpha_1 x^{n-1} + \cdots + (-1)^n \alpha_n$$

是 $F(\alpha_1, \cdots, \alpha_n)[x]$ 中多项式，它的分裂体是 F 的超越体 $F(x_1, \cdots, x_n)$. 我们知道，不使 $F(\alpha_1, \cdots, \alpha_n)$ 中任意元变动的 $F(x_1, \cdots, x_n)$ 的自同构，显然不使 $h(x)$ 的任意系数 α_i 变动，因此它把 $h(x)$ 的零点仍然变为 $h(x)$ 的零点，所以它决定 $x_1, \cdots, x_n$ 的一个排列. 反过来，因为 $x_1, \cdots, x_n$ 都是未定元，也就是说，它们都是记号，我们容易知道，它们的任意一个排列诱导出 $F(x_1, \cdots, x_n)$ 的一个自同构，这自同构不使 $\alpha_1, \cdots, \alpha_n$ 变动，因此也不使 $F(\alpha_1, \cdots, \alpha_n)$ 中任意元变动，所以 $x_1, \cdots, x_n$ 的任意一个排列决定一个不使 $F(\alpha_1, \cdots, \alpha_n)$ 中任意元变动的 $F(x_1, \cdots, x_n)$ 的自同构. 于是 $F(x_1, \cdots, x_n)$ 关于 $F(\alpha_1, \cdots, \alpha_n)$ 的伽罗瓦群是 n 个文字 $x_1, \cdots, x_n$ 上的对称群 S_n.

假如我们能够证明 $K = F(v_1, \cdots, v_n)$ 与 $F(x_1, \cdots, x_n)$ 的同构是 $F(u_1, \cdots, u_n)$，$F(\alpha_1, \cdots, \alpha_n)$ 的延长，那末 $F(u_1, \cdots, u_n)$ 的扩张体 $F(v_1, \cdots, v_n)$ 可以看成是 $F(\alpha_1, \cdots, \alpha_n)$ 的扩张体 $F(x_1, \cdots, x_n)$，因此 $K = F(v_1, \cdots, v_n)$ 关于 $F(u_1, \cdots, u_n)$ 的伽罗瓦群就可以看成是 $F(x_1, \cdots, x_n)$ 关于 $F(\alpha_1, \cdots, \alpha_n)$ 的伽罗瓦群. 于是 $f(x)$ 的伽罗瓦群就是对称群 S_n，所以定理就告成立.

我们先证明下面多项式 $g(\alpha_1, \cdots, \alpha_n)$ 的一个性质，以备引用.

假如 $\alpha_1, \cdots, \alpha_n$ 的多项式 $g(\alpha_1, \cdots, \alpha_n) = 0$，那末 $g(\alpha_1, \cdots, \alpha_n)$ 的系数全都是零. 这是因为，由 $g(\alpha_1, \cdots, \alpha_n) = 0$，我们有

$$g(\sum x_i, \sum x_i x_j, \cdots) = 0,$$

因为 x_i 是未定元，用 v_i 来代替 x_i 就得到

$$g(\sum v_i, \sum v_i v_j, \cdots) = 0,$$

即 $$g(u_1, u_2, \cdots, u_n) = 0.$$

但 $u_1, u_2, \cdots, u_n$ 是 n 个未定元，所以 $g(u_1, \cdots, u_n)$ 的系数全都是零，因此 $g(\alpha_1, \cdots, \alpha_n)$ 的系数完全是零.

现在来证明上面两个体的延长.

我们命 $F(\alpha_1, \cdots, \alpha_n)$ 中元 $f(\alpha_1, \cdots, \alpha_n)/g(\alpha_1, \cdots, \alpha_n)$ 与 $F(u_1, \cdots, u_n)$ 中元 $f(u_1, \cdots, u_n)/g(u_1, \cdots, u_n)$ 对应，即

$$f(u_1, \cdots, u_n)/g(u_1, \cdots, u_n) \to f(\alpha_1, \cdots, \alpha_n)/g(\alpha_1, \cdots, \alpha_n).$$

这对应显然是 $F(u_1, \cdots, u_n)$ 射到 $F(\alpha_1, \cdots, \alpha_n)$ 上的同态，并且还是可逆的. 这是因为，假如

$$f(\alpha_1, \cdots, \alpha_n)/g(\alpha_1, \cdots, \alpha_n) = f_1(\alpha_1, \cdots, \alpha_n)/g_1(\alpha_1, \cdots, \alpha_n),$$

那末

$$f(\alpha_1, \cdots, \alpha_n)g_1(\alpha_1, \cdots, \alpha_n) - f_1(\alpha_1, \cdots, \alpha_n)g(\alpha_1, \cdots, \alpha_n) = 0,$$

因此由上面证得的性质，

$$f(u_1, \cdots, u_n)g_1(u_1, \cdots, u_n) - f_1(u_1, \cdots, u_n)g(u_1, \cdots, u_n) = 0,$$

所以

$$f(u_1, \cdots, u_n)/g(u_1, \cdots, u_n) = f_1(u_1, \cdots, u_n)/g_1(u_1, \cdots, u_n),$$

于是 $$F(u_1, \cdots, u_n) \cong F(\alpha_1, \cdots, \alpha_n).$$

这时 α_i 与 u_i 对应，即 $h(x)$ 的系数与 $f(x)$ 的系数对应. 但 $F(v_1, \cdots, v_n)$, $F(x_1, \cdots, x_n)$ 分别是 $f(x)$, $h(x)$ 的分裂体，根据 §4.6 定理 3,

$$F(v_1, \cdots, v_n) \cong F(x_1, \cdots, x_n),$$

并且它们是 $F(u_1, \cdots, u_n)$, $F(\alpha_1, \cdots, \alpha_n)$的延长，因此定理得证.

我们知道对称群 S_n，当 $n \leqslant 4$ 时是可解群，当 $n \geqslant 5$ 时不是可解群. 所以当 F 的特征数不是 2 或 3 时，$F[x]$ 中 5 次以下的多项式都能够用根号解出. 4 次以上的一般多项式不能用根号解出，即

定理 2 n 次一般多项式当 $n \geqslant 5$ 时，不能够用根号解出.

要注意的是，这里讨论的虽然是一般多项式，但是 4 次以上的多项式即使系数是整数的也不一定都能够用根号解出，后面 § 6.6 习题 2 就是一个显明的例子.

习 题 6.5

1. 假如已知 $n \geqslant 5$ 时交代群 A_n 是单群，试用这性质证明对称群 S_n 不是可解群.

§ 6.6 质数次既约多项式的解

我们已经知道，多项式的伽罗瓦群是关于它零点的对称群，或者是对称群的子群. 既约多项式的伽罗瓦群是关于它零点的可迁群. 下面我们来讨论怎样的可迁群才是可解群?

我们先介绍一个定义以备引用.

假设 σ 是数字 $1, 2, \cdots, n$ 的排列，如果有整数 $a(\not\equiv 0(n))$, b 存在，使

$$\sigma(i) \equiv ai + b(n), \quad i = 1, 2, \cdots, n,$$

那末 σ 叫做关于 n 的**线性变换**.

下面是我们需要的定理.

定理 1 假定 $f(x)$是 $F[x]$ 中质数 p 次的既约多项式，它的伽

罗瓦群 G 是$\{1, 2, \cdots, p\}$的可迁群，那末 G 是可解群的必要充分条件是：把 $1, 2, \cdots, p$ 的顺序适当改写后，G 中任意元是关于 p 的线性变换，并且 G 包含所有 $a=1(p)$ 的线性变换

$$\sigma^b(i)\equiv i+b(p),\quad b=1, 2, \cdots, p.$$

证明　我们先用数学归纳法来证明必要性.

假如 G 是可解群，

$$G=G_0\supset G_1\supset\cdots\supset G_k\supset G_{k+1}=E$$

是它的正规群列，并且 G_{i-1}/G_i是可换群，这时我们可以假定 G_k是循环群，因为如果它不是循环群，任取它的一个循环子群插入 G_k, G_{k+1} 之间就能成为这样的正规群列.

因为 G 是 $\{1, 2, \cdots, p\}$ 的可迁群，G_1 是 G 的正规子群，由 §5.6 定理 2, G_1 也是 $\{1, 2, \cdots, p\}$ 的可迁群，因此 $G_2, \cdots, G_k$ 都是 $\{1, 2, \cdots, p\}$ 的可迁群．假定 σ 是 G_k 的生成元，也就是 $G_k=(\sigma)$，那末 σ 是 p 个数字的循环排列．这是因为，如果 $\sigma=(1ij\cdots m)(n\cdots q)$, σ 的乘幂只能把 1 变为 $1, i, j, \cdots, m$，而不能把 1 变为$n, \cdots, q$，这与 $G_k=(\sigma)$ 是可迁群的性质不合，因此如果把 $1, 2, \cdots, p$ 的顺序适当改写，我们就有

$$\sigma(i)\equiv i+1(p),$$

于是

$$\sigma^r(i)\equiv i+r(p),\quad r=1, 2, \cdots, p.$$

再假设 τ 是 G_{k-1} 中任意元，因为 G_k 是 G_{k-1} 的正规子群，所以 $\tau\sigma\tau^{-1}\in G_k$，我们命

$$\tau\sigma\tau^{-1}=\sigma^a,\quad \tau(i)=j,$$

因此

$$\tau\sigma\tau^{-1}(j)=\sigma^a(j)\equiv j+a(p),$$

于是

$$\tau\sigma(i)=\sigma^a\tau(i)\equiv\tau(i)+a(p).$$

也就是说，对任意 i，我们有

$$\tau(i+1)\equiv\tau(i)+a(p).$$

假如令 $\tau(0)\equiv b$，那末

$$\tau(1)\equiv b+a,\quad \tau(2)\equiv\tau(1)+a=b+2a,\quad \cdots,$$

一般
$$\tau(i)\equiv b+ai,$$

这就是说，G_{k-1} 中任意元是关于 p 的线性变换．因为当 $a\not\equiv 1(p)$ 时，有适合 $b+ai\equiv i(p)$，即 $(a-1)i\equiv -b(p)$ 的数 i 存在，所以只有 $\tau(i)\equiv b+i(p)$ 使任意数字变动，但 $\tau=\sigma^b$，因此 G_{k-1} 中使任意数字变动的排列是 G_k 中排列，也就是说，G_{k-1} 中任意 p 项循环排列是 G_k 中排列．

现在我们假设 G_{k-a} 有 G_{k-1} 的性质，即 G_{k-a} 中任意排列是关于 p 的线性变换，并且 G_{k-a} 中任意 p 项循环排列是 G_k 中排列．如果 τ 是 G_{k-a-1} 中任意排列，因为 σ 是 p 项循环排列，由 §2.2 习题 10，$\tau\sigma\tau^{-1}$ 是 G_{k-a} 中 p 项循环排列，因此在 G_k 中．于是 $\tau\sigma\tau^{-1}=\sigma^a$，即 $\tau\sigma=\sigma^a\tau$．同上面一样，我们有 $\tau(i)\equiv ai+b(p)$，因此 G_{k-a-1} 中任意元是关于 p 的线性变换，并且其中任意 p 项循环排列是 G_k 中排列，由归纳法我们得知必要条件成立．

下面我们来证明充分性．

假定 G 是由关于 p 的线性变换形成的群，N 是其中所有形状象 $\sigma^b(i)\equiv i+b(p)$，$b=1,2,\cdots,p$，的线性变换形成的可换子群，那末 G 中使任意数字变动的排列都是 N 中排列，也就是说，G 中任意 p 项循环排列都在 N 中．但用 G 中任意排列把 N 中任意排列变形（§24）得到的排列仍然是 p 项循环排列，因此也是 N 中排列，所以 N 是 G 的正规子群．假如 $\tau(i)\equiv ai+b$ 是 G 中任意元，那末在陪集 τN 中有

$$\tau\sigma^r(i)\equiv ai+ar+b\equiv ai(p),$$

这里 $ar+b\equiv 0(p)$，如果 $\tau(i)\equiv ai$，$\tau'(i)\equiv a'i$，我们就有 $\tau\tau'(i)\equiv aa'i$．因此，假如命 τ 与 a 对应，我们很容易证明这对应是 G/N 射到 $Z-(p)$ 的乘群内的同构，所以 G/N 与 $Z-(p)$ 的乘群的子群同构．于是 G/N 是可换群．因为 G/N 及 N 都是可换群，所以 G

是可解群，因此定理成立.

一个关于质数 p 的线性变换 $\sigma(i)\equiv ai+b(p)$ 除不动排列外，最多只能够使一个数字不变动. 这是因为，同余式 $i\equiv ai+b(p)$，即

$$(a-1)i\equiv -b(p),$$

除 $a=1$, $b=0$ 外，最多只能够有一个解. 因此假如这时线性变换能够使两个数字不变动，那末它就使任意数字不变动了.

下面是一个常常引用的重要定理.

定理 2 假如系数是实数的质数次既约多项式 $f(x)$ 能够用根号解出，那末它的零点只有一个是实数或者全部都是实数.

证明 因为 $f(x)$ 的分裂体 K 是复数体的子体，显然其中任意数与它的共轭对应是不使 K 中实数变动的 K 的自同构，因此它是 $f(x)$ 的伽罗瓦群 G 中元. 假如 $f(x)$ 的分裂体中含有复数，那末这元就不是 G 的单位元，因此它不能使两个实数不变动，这就是说，假如 $f(x)$ 的零点不都是实数，它只能有一个零点是实数，因此定理得证.

习　题　6.6

1. 5次实系数既约多项式如果只有三个实根，它就不能够用根号解出.
2. 试证多项式 x^5-4x+2 不能够用根号解出.

§6.7　用圆规与直尺的作图

假如我们已经知道平面上有穷个初等几何图形(点、直线、圆等)，要求用圆规及直尺来作适合已给条件的初等几何图形，这要求在什么条件下才能实现？当然这条件是包含那些已知初等几何图形的. 这节我们就是解答这问题.

我们知道在用圆规及直尺作图的过程中，在已知范围内可以任意挑选一点，过两点可以作一直线，已知圆心及半径可以作一圆．假如两直线、两圆或一直线一圆能够作出，那末它们的交点也能够作出．一个初等几何图形能够作出，只不过是重复引用上面的方法作出一些适当的点，直线，圆罢了．

因为直线同圆都可以用点来决定，所以用圆规与直尺的作图问题可以看成是由已知点作出适合某些条件的点的问题．假如我们引用坐标，把点换成数，那末作点的问题就变为作数的问题了．假如数 $a, b, c, \cdots$ 是决定已知图形的点的坐标，因为它们中任意两数的和、差、积、商都能作出，所以体 $F=Q(a, b, c, \cdots)$ 中数都能够作出，这里 Q 是有理数体．

现在我们来讨论初等几何图形能够用圆规与直尺作出的条件．

我们知道，一点如果能够任意挑选，我们可以假定它的坐标是有理数．过坐标是 F 中数的两点的直线，它的方程的系数也是 F 中数，因此这样的两条直线的交点的坐标又是 F 中数．如果圆上的三个点，或一个点同它的圆心，它们的坐标都是 F 中数，那末这圆的方程的系数也是 F 中数．但是方程的系数是 F 中数的两圆或一圆一直线，它们交点的坐标一般含有 F 中数的平方根，所以不一定是 F 中数．于是假如数 x 能够作出，也就是说，x 是方程的系数为 F 中数的某些直线及圆的交点，那末 x 能够用 F 中数的有理运算及平方根号表示．反过来显然也成立，这是因为我们根据 $1:b=b:a$ 可以作出已知数 a 的平方根 $b=\sqrt{a}$．于是我们有

定理 1 数 x 能够用圆规与直尺作出的必要充分条件是：它能够用 F 中数的有理运算及平方根号表示．

现在我们要进一步问，怎样的数才能够用 F 中数的有理运算及平方根来表出？我们又如何来判别？

假如数 x 能够用 F 中数的有理运算及平方根表示，那末它就在陆续添加平方根于 F 形成的可换体中. 同 §6.4 中所讨论的一样，这体可以再用平方根来扩张使它成为 F 的正规体 K，即

$$K=F_m\supset F_{m-1}\supset\cdots\supset F_0=F,$$

这里 F_i 是 F_{i-1} 中纯多项式 x^2-a_i 的分裂体，因为 $(F_i:F_{i-1})=2$，根据 §4.4 定理 4，我们有

$$(K:F)=(F_m:F_{m-1})\cdots(F_1:F)=2^m.$$

反过来，假如 x 在 F 的正规体 K 中，并且 $(K:F)=2^m$，那末 K 关于 F 的伽罗瓦群 G 的元数是 2^m，因此由 §5.3 定理 8，G 是可解群. 我们知道有穷群有合成群列，元数是 p^n 的群只有 $n=1$ 时才是单群，因此 G 有商群的元数都是 2 的合成群列

$$K=F_m\supset F_{m-1}\supset\cdots\supset F_0=F,$$

这时 $(F_i:F_{i-1})=2$，所以 x 能够用 F 中数的有理运算及平方根表出. 因此我们有

定理 2 数 x 能够用圆规与直尺作出的必要充分条件是它在关于 F 次数为 2^m 的正规体中.

下面我们来讨论三个古典的初等几何作图问题，以作结束.

首先谈圆的求积问题. 假如我们取圆的半径为 1，那末求作与圆的面积相等的正方形就是求作 π，但 π 是超越数[5]，显然不能用有理数及有理数的平方根表示. 因此它不能用圆规与直尺作出.

其次谈立方倍积问题. 假如我们取立方体的一边长作为 1，那末要作的数 x 应适合条件 $x^3-2=0$，这多项式的零点不是有理数. 如果命 α 是它的零点，那末 $(Q(\alpha):Q)=3$，所以 α 不在有理数体 Q 的 2^m 次扩张体中，因此 x 不能够用圆规与直尺作出.

最后谈任意角三等分问题. 假如 α 是任意角，θ 是所求角，因为 $\alpha=3\theta$，由三角公式，得

$$\cos\alpha=\cos 3\theta=4\cos^3\theta-3\cos\theta.$$

命 $\cos\alpha=\frac{a}{2}$, $\cos\theta=\frac{x}{2}$, 那末 x 所适合的条件是

$$4\left(\frac{x}{2}\right)^3-3\cdot\frac{x}{2}=\frac{a}{2},$$

即

$$x^3-3x-a=0.$$

如果取 $\alpha=60^\circ$, 那末 $a=1$. 但 $x^3-3x-1=0$ 没有有理数的零点, 假如把它的零点添加于有理数体 Q 得到的体是 K, 那末 $(K:Q)=3$, 所以 x 不能用圆规与直尺作出. 因此 θ 也不能够用圆规与直尺作出.

参考文献

[1] Mccormick, Gravill, A theorem on finite abelian groups, Amer. Math. Monthly, 67 (1960), 670.

[2] T. Nakayama (中山正), Generalized Galois theory of rings with minimum condition, I, Amer. Jour. of Math., 73(1951), 1～12; II, Amer. Jour. of Math., 77 (1955), 1～16.

[3] (1) E. Artin, Galois Theory (1946), 64～65.
(2) P. Wilker, Über die Zwischenkörper einfacher Algebraisher Erweiterungen, Math. Ann., 124 (1952), 289～290.

[4] (1) M. Deuring, Galoische Theorie und Darstellungstheorie, Math. Ann., 107 (1932), 140～144.
(2) E. Artin, Galois Theory (1946), 66～67.
(3) J. W. S. Gasseis and G. E. Wall, The normal basis theorem, Jour. of London Math. Soc., 25 (1950), 259～264.

[5] I. Niven, A simple proof that π is irrational, Bull, Amer. Math. Soc., 53 (1947), 509.

第七章

环　　论

环构造的研究可以说是从本世纪初1908年魏特邦关于有穷次代数构造的著名论文[1]开始．经过一个较长时间，进展不大；到了三十年代魏特邦定理才得到推广．1927年阿丁提出了用极小条件来区别环．阿丁把魏特邦定理推广到满足极小条件的环[2]，基本上解决了满足极小条件环的构造问题，因此满足极小条件的环叫做阿丁环．在四十年代开始研究不满足极小条件的环．1945年贾柯勃逊创造根基理论，把魏特邦定理进一步推广到不满足极小条件的环[3]，建立了一般环的构造理论，在五十年代提出了各种不同的根基理论[4]，互有短长．但一般仍以贾柯勃逊理论为主．

目前介绍环构造书籍为数不少，其中内容丰富涉及面又广的要以1956年贾柯勃逊所著环构造[5]为最，只是起点较高，初学难以领会．此外，1969年卡泼伦斯基的体与环[6]也是一本好书，内容新颖，论证严明，可供参考．

这章主要讨论环的构造，分7节，前4节讨论满足极小条件环的构造，后三节根据贾柯勃逊根基，讨论一般环的构造．

§7.1　极小条件

1927年阿丁把1908年魏特邦的有穷次代数构造定理推广到满足极小条件的环，这些定理叫做魏特邦-阿丁定理．这章前四节

主要是介绍这些定理．为了叙述方便，今后两节先介绍基本概念及性质，以备引用．

假定 R 是环，如果它的任意左理想子环列

$$L_1 \supset L_2 \supset \cdots \supset L_n \supset \cdots, \quad L_i \text{ 是 } R \text{ 的左理想子环},$$

只有有穷项，也就是说，对于任意含无穷项的左理想子环列

$$L_1 \supsetneqq L_2 \supsetneqq \cdots \supsetneqq L_n \supsetneqq \cdots,$$

必定有一个正整数 m 存在，自 m 项后的所有左理想子环都相等，即

$$L_m = L_{m+1} = \cdots,$$

那末 R 叫做满足(左理想子环)**降链条件**．

假如 R 是满足降链条件的环，那末在它的任意左理想子环的集合中，有不包含这集合中其他左理想子环的左理想子环，也就是说，任意左理想子环集合包含极小左理想子环．这是因为，假如 L_1 是这集合中左理想子环，如果它不是极小左理想子环，那末这集中有包含于 L_1 的左理想子环 L_2，于是我们有 $L_1 \supset L_2$．如果 L_2 又不是极小左理想子环，我们又有 $L_1 \supset L_2 \supset L_3$，这样继续下去，我们就得到左理想子环列

$$L_1 \supset L_2 \supset L_3 \supset \cdots \supset L_i \supset \cdots,$$

因为它只能有有穷项，所以最后的 L_m 就不包含这集中其他左理想子环，因此 L_m 就是极小左理想子环．一个环 R，如果它的任意左理想子环集都有极小理想子环，我们就说 R 满足(左理想子环)**极小条件**．因此，一个环如果满足降链条件，它也满足极小条件．反过来，如果环满足极小条件，显然它也满足降链条件．极小条件是降链条件的另一表达形式．

譬如有穷环显然是满足极小条件的环．再因为体只有两个左理想子环，所以体也是满足极小条件的环．又假如 A 是可换体 F 上的代数，因为 A 的左理想子环 L_i 是 A 的子空间，并且当 $L_i \supset L_j$ 时，L_i 的维数大于 L_j 的维数，所以 A 满足极小条件．但整数环不

满足极小条件，因为

$$(m)\supset(2m)\supset(2^2m)\supset\cdots$$

就是含无穷项的理想子环列．同样，主理想子环环以及多项式环都不满足极小条件，所以极小条件是一个很强的条件，就是最普通的环有的也不满足这条件．

满足极小条件的环 R 假如看成 R 空间，那末这空间的维数是有穷的．这维数又常常叫做 R 的长．

下面我们介绍几个基本性质．

我们知道，假如环 $R=R_1+\cdots+R_m$，如果 R 满足极小条件，因为 R_i 的左理想子环也是 R 的左理想子环，所以 R_i 也满足极小条件．反过来也基本成立．

定理 1 假定 R 是有单位元的环，$R=R_1+\cdots+R_n$，如果子环 $R_1,\cdots,R_n$ 都满足极小条件，那末 R 也满足极小条件．

证明 假定$\{L_i\}$是 R 的任意左理想子环集合，根据§5.4定理5，我们有

$$L_i=L_{i1}+\cdots+L_{in},\quad L_{ij}=L_i\cap R_j,$$

因为$\{L_{i1}\}$是 R_1 的左理想子环集合，由极小条件，它有极小理想子环 L_1^*．命$\{L_i\}$中所有与 R_1 的交集是 L_1^* 的左理想子环是$\{L_i'\}$，因为$\{L_i'\cap R_2\}$是 R_2 的左理想子环，又由极小条件，它有极小左理想子环 L_2^*．再命$\{L_i'\}$中所有与 R_2 的交集是 L_2^* 的是$\{L_i''\}$．这样继续下去，最后假如$\{L_i^{(n-2)}\}$中所有与 R_n 的交集是 L_{n-1}^* 的是$\{L_i^{(n-1)}\}$，它的极小左理想子环是 L_n^*．于是

$$L^*=L_1^*+\cdots+L_n^*$$

就是$\{L_i\}$的极小左理想子环，这是因为，如果$\{L_i\}$中有 $L^{**}\subset L^*$，那末

$$L^{**}=L_1^{**}+\cdots+L_n^{**},\quad L_i^{**}=L^{**}\cap R_i.$$

于是 $L_i^{**}\subseteq L_i^*$，显然其中必有某 $L_k^{**}\subset L_k^*$，这与 L_k^* 是$\{L_i^{(k-1)}\cap R_k\}$

的极小左理想子环的假设不合. 因此 L^* 是 $\{L_i\}$ 的极小左理想子环,所以定理成立.

定理 2　假定环 R 满足极小条件, 那末同余环 $\bar{R}=R-N$ 也满足极小条件,这就是说,满足极小条件环的同态象也是满足极小条件的环.

证明　假定
$$\bar{L}_1\supseteq\bar{L}_2\supseteq\cdots\supseteq\bar{L}_n\supseteq\cdots$$
是同余环 $\bar{R}$ 的任意左理想子环列,因为 $R\sim\bar{R}$, 所以 $\bar{L}_i$ 在 R 的完全象源 L_i 是 R 的左理想子环, 因此
$$L_1\supseteq L_2\supseteq\cdots\supseteq L_n\supseteq\cdots$$
是 R 的左理想子环列. 但 R 满足极小条件, 所以 $L_m=L_{m+1}=\cdots$. 于是
$$\bar{L}_m=\bar{L}_{m+1}=\cdots,$$
这就是说, $\bar{R}$ 满足极小条件,所以定理成立.

定理 3　假定环 R 有单位元, 并且满足极小条件, 那末 R 的有穷维空间也满足极小条件.

证明　假定 $V=Ru_1+\cdots+Ru_n$,我们容易得知 $r\to ru_i$ 是 R 看成 R 空间时射到 R 空间 Ru_i 上的同态, 因此 $R\sim Ru_i$. 因为 R 满足极小条件, 由定理 2, Ru_i 也满足极小条件, 再由定理 1 得知 V 满足极小条件,所以定理成立.

特别,假如 K 是体,那末全矩阵环 K_n 满足极小条件.

在满足极小条件的环中具备很多重要的性质.

我们知道,元数是有穷的无零因子环是体 (§3.2). 一般我们有

定理 4　满足极小条件的无零因子环是体.

证明　假定 R 是满足极小条件的无零因子环, a 是 R 中非零元,对于左理想子环列
$$Ra\supset Ra^2\supset\cdots,$$

根据极小条件,有整数 n 存在,使 $Ra^n=Ra^{n+1}$, 因此 $ba^n=ca^{n+1}$, 但 $a^n\neq 0$, 所以 $ca=b$, 由 § 3.2 定理 2, 于是 R 是体. 所以定理成立.

我们知道,在可换环中质理想子环不一定是极大理想子环,但在满足极小条件环中却是如此,即

定理 5 在满足极小条件的可换环中, 质理想子环是极大理想子环.

证明 假定 P 是满足极小条件环 R 的质理想子环,那末 $R-P$ 是无零因子环, 又因为 $R-P$ 满足极小条件, 由上定理, $R-P$ 是体,因此 P 是极大理想子环. 于是定理成立.

在上面的讨论中,假如把左理想子环换成右理想子环,我们就得到满足右理想子环极小条件的类似理论. 但要注意的是, 同一个环, 它满足左理想子环的极小条件不一定就满足右理想子环的极小条件. 譬如, 假定 A 是基础体为有理数体 Q, 底元为 e, a 的代数,即

$$A=Qe+Qa,$$

其中
$$e^2=e,\ a^2=0,\ ea=a,\ ae=0,$$

因为 A 的左理想子环是 A 的子空间,所以它满足左理想子环的极小条件. 假如 (m) 是 Q 中所有整数 m 的倍数形成的加群, 因为 A 中任意元右乘 $(m)a$ 都成为零, 所以 $(m)a$ 是 A 的右理想子环, 因此 A 的右理想子环列

$$(m)a\supset(2m)a\supset(2^2m)a\supset\cdots$$

含有无穷项. 所以 A 不满足右理想子环的极小条件.

习 题 7.1

1. 假定 V 是环 R 空间, 试证 R 中所有适合 $xV=0$ 的元 x 形成 R 的理想子环.

2. 假定 V 是环 R 的既约空间, x 是 R 中任意元, 试证 $Rx=V$ 或 $Rx=0$.

3. 假定 V 是 R 空间，并且 V 中任意非零元不能够被 R 中所有元零化，如果 V 是它的既约子空间 $V_1, \cdots, V_m$ 的直和，同时又是既约子空间 $W_1, \cdots, W_n$ 的直和，即 $V=V_1+\cdots+V_m=W_1+\cdots+W_n$，那末 $m=n$.

4. 假如 R 不满足极小条件，全矩阵环 R_n 是否也不满足极小条件？

§7.2 幂零理想子环

从§3.7我们知道，假定 L 是环 R 的左理想子环，如果其中任意元都是幂零元，就叫 L 做幂零元左理想子环，如果 L 的某乘幂是零理想子环，即有某正整数 m 存在，使

$$L^m=0,$$

那末 L 叫做幂零左理想子环. 显然，幂零左理想子环是幂零元左理想子环，但幂零元左理想子环不一定是幂零左理想子环，因为象上面那样的正整数 m 不一定存在.

在可换环中，两个幂零元的和仍然是幂零元. 在一般环中这性质不成立，即两个幂零元左理想子环的和不一定是幂零元左理想子环. 但对于幂零左理想子环，我们有

定理 1 假定 L_1、L_2 是环 R 的幂零左理想子环，那末它们的和 (L_1, L_2) 也是 R 的幂零左理想子环.

证明 假定

$$L_1^{m_1}=0, \quad L_2^{m_2}=0.$$

根据结合律及分配律，我们把 L_1, L_2 的和 (L_1, L_2) 的 m_1+m_2-1 乘幂 $(L_1, L_2)^{m_1+m_2-1}$ 展开，就成为每项含有 m_1+m_2-1 个因子的展开式. 在这展开式的任意一项中，如果含 L_1 的个数小于 m_1，那末它含 L_2 的个数就不小于 m_2. 因为 L_1, L_2 都是 R 的左理想子环，当它含 L_1 的个数不小于 m_1 时，我们就有

$$\cdots L_1\cdots L_1\cdots L_1\cdots\subseteq\cdots L_1^{m_1}\cdots=0,$$

当它含 L_2 的个数不小于 m_2 时，我们有

$$\cdots L_2\cdots L_2\cdots L_2\cdots \subseteq \cdots L_2^{m_2}\cdots = 0,$$

这就是说，展开式中任意项都是零理想子环，所以 $(L_1, L_2)^{m_1+m_2-1}=0$，于是定理成立.

显然，有穷个幂零左理想子环的和仍然是幂零左理想子环，但无穷个幂零左理想子环的和一般只能是幂零元左理想子环而不是幂零左理想子环. 这是因为，假如 a 是无穷个幂零左理想子环的和 L 中任意元，根据定义，我们得知 a 是某有穷个幂零左理想子环的和中元，因此 a 是幂零元，但这些乘幂不一定有最大数，所以 L 不是幂零左理想子环.

在什么条件下幂零元左理想子环又是幂零左理想子环？1939年霍布金斯(C. Hopkins)给出了一个充分条件：在满足极小条件环中，幂零元左理想子环又是幂零左理想子环[7]. 1942年布劳尔(R. Brauer, 1901～)提出了下面要求更强的定理[8]，引用这定理我们立即推得霍布金斯定理.

定理 2 假定 R 是满足极小条件环，L 是 R 的左理想子环，如果 L 不是幂零左理想子环，那末 L 中有幂等元，因此 L 不是幂零元左理想子环.

证明 我们先在 L 中找出一个适当的非幂零元.

因为 R 满足极小条件，所以 L 中所有 R 的非幂零左理想子环集合有极小左理想子环. 假定 L_1 是这极小左理想子环. 因为 $L_1^2\subseteq L_1$，并且 L_1^2 又是 L 中 R 的非幂零左理想子环，所以 $L_1^2=L_1$. 再 L_1 中所有满足 $L_1L'\neq 0$ 的 R 的左理想子环 L' 的集合，由极小条件，它也有极小左理想子环 L_2，因此 $L_1L_2\neq 0$. 于是在 L_2 中有元 u 使

$$L_2u\neq 0.$$

又因为 L_1u 是 L_1 中 R 的左理想子环，并且 $L_1\cdot L_1u=L_1u\neq 0$，

所以 $L_1u=L_1$. 因此在 L_1 中有满足

$$eu=u$$

的元 e. 于是对于任意正整数 n, 我们有 $e^nu=u$, 因为 $u\neq0$, 所以 e 不是幂零元. 这就是说, L_1 中有非幂零元 e.

再我们引用这非幂零元 e 来求幂等元.

我们容易知道, L_1 中所有满足 $xu=0$ 的元 x 形成 R 的左理想子环 L_1', 因为 $e^2u=eu$, 即 $(e^2-e)u=0$, 所以 $e^2-e\in L_1'$. 又因为 $L_1u\neq0$, 所以 $L_1'\subset L_1$, 但 L_1 是 R 的非幂零极小左理想子环, 因此 L_1' 是幂零左理想子环. 于是 $e^2-e=t$ 是幂零元. 我们命 $t^n=0$, 如果 $n=1$, 那末 $e^2=e$, 即 e 是幂等元. 所以这时定理成立, 如果 $n\neq1$, 命

$$e_1=e-2et+t,$$

由计算我们容易得知

$$e_1^2=e_1+4t^3-3t^2,\text{ 即 }e_1^2-e_1=4t^3-3t^2.$$

因此 $e_1^2-e_1=t_1$ 又是幂零元. 命 $t_1^{n_1}=0$, 显然 $n>n_1$. 如果 $n_1=1$, 那末 $e_1^2=e_1$, 即 e_1 是幂等元. 所以这时定理成立. 如果 $n_1\neq1$, 命

$$e_2=e_1-2e_1t_1+t_1,\quad t_2=e_2^2-e_2,$$

重复引用上面方法, 我们就得到幂零元列 $t,\ t_1,\ t_2,\cdots$, 因为它们的乘幂 $n>n_1>n_2>\cdots$, 所以最后得 $n_m=1$. 于是 $t_m=e_m^2-e_m=0$, 即 e_m 是幂等元. 因此定理成立.

于是在满足极小条件的环中, 幂零元左理想子环是幂零左理想子环. 因此在满足极小条件的环中, 所有幂零左理想子环的和仍然是幂零左理想子环. 这最大的幂零左理想子环在讨论环的构造时起着重大的作用, 因此我们有

定义　假定 R 是满足极小条件的环, 那末 R 中所有幂零左理想子环的和是 R 中最大幂零左理想子环, 叫做 R 的**根基**.

要注意的是, 满足极小条件环 R 的根基 N 中元都是幂零元,

但 R 的幂零元不一定都在 N 中. 譬如全矩阵环 Q_2 的根基是零(§7.3 定理 7), 但$\begin{pmatrix}0&1\\0&0\end{pmatrix}$,$\begin{pmatrix}0&0\\1&0\end{pmatrix}$都是幂零元. 假如 R 是可换环, a 是 R 的幂零元, 那末 ra, $r\in R$ 也是幂零元, 因此由 a 生成的理想子环是幂零理想子环, 所以 $a\in N$. 于是 N 是 R 中所有幂零元形成的理想子环.

定理 3 假定 R 是满足极小条件的环, N 是它的根基, 那末 R 中元 $a\in N$ 的必要充分条件是: a 及 ra 都是幂零元, 这里 r 是 R 中任意元.

证明 因为 a 及所有的 ra 形成 R 的左理想子环 L, 如果 a 及 ra 都是幂零元, 那末 L 是幂零元理想子环, 所以 $L\subseteq N$, 因此 $a\in N$. 反过来, 假如 $a\in N$, 那末 $ra\in N$, 因此 a 及 ra 都是幂零元, 于是定理成立.

下面是根基的两个基本性质.

定理 4 环 R 的根基 N 是 R 的幂零理想子环, 它既包含 R 的所有幂零左理想子环, 也包含 R 的所有幂零右理想子环.

证明 假定 K 是 R 的幂零右理想子环, 同定理 1 的证明一样, 我们容易证明 RK 是 R 的幂零理想子环, 因此它们的和(K, RK)也是 R 的幂零理想子环, 于是$(K, RK)\subseteq N$, 所以 $K\subseteq N$, 这就是说, N 包含 R 的所有幂零右理想子环.

再因为 N 是 R 的幂零左理想子环, 我们可以同样证明 NR 是 R 的幂零理想子环, 因此 $NR\subseteq N$, 这就是说, N 是 R 的理想子环. 所以定理成立.

我们知道, 在满足左理想子环极小条件的环中, 任意幂零元左理想子环是幂零左理想子环. 在满足右理想子环极小条件的环中, 任意幂零元右理想子环当然是幂零右理想子环. 因此一个环 R, 如果满足左理想子环的极小条件, 但不满足右理想子环的极小条件, 那末它的最大幂零左理想子环只包含 R 的所有幂零元左理

想子环，不包含 R 的所有幂零元右理想子环．如果 R 既满足左理想子环的极小条件，又满足右理想子环的极小条件，那末它的最大幂零左理想子环包含 R 的所有幂零元左理想子环，也包含 R 的所有幂零元右理想子环．因此 R 的最大幂零左理想子环与最大幂零右理想子环是一致的．

一个满足极小条件的环，如果它的根基是零，就叫做**半单纯环**；如果它的根基是自身，就叫做**根基环**．显然幂零环是根基环，当然，根基环也是幂零环．因为单位元不是幂零元，所以有单位元的环不是根基环．

定理 5　假定 N 是环 R 的根基，那末 $\bar{R}=R-N$ 的根基是零，也就是说，$\bar{R}$ 是半单纯环．

证明　因为 R 满足极小条件，由 §7.1 定理 2，$\bar{R}$ 也满足极小条件．再假定 $\bar{L}$ 是 $\bar{R}$ 的幂零左理想子环，$\bar{L}^m=\bar{0}$，L 是 $\bar{L}$ 在 R 的完全象源，那末 $L^m\equiv 0(N)$，即 $L^m\subseteq N$．但 N 是 R 的幂零理想子环，$N^n=0$，于是 $L^{mn}=0$，因此 L 是 R 的幂零左理想子环，所以 $L\subseteq N$．于是 $\bar{L}=0$，这就是说，$\bar{R}$ 中只有零理想子环是幂零左理想子环，因此 $\bar{R}$ 的根基是零，所以 $\bar{R}$ 是半单纯环，于是定理成立．

习　题　7.2

1．试求 3 次代数 $A=Fu_1+Fu_2+Fu_3$ 的根基，A 的乘法表是

	u_1	u_2	u_3
u_1	u_1	0	u_3
u_2	0	u_2	0
u_3	0	u_3	0

2．试证同余环 $Z-(m)$ 的根基是零的必要充分条件为：m 不能用质数的平方整除．

3．试证根基是零的环，它的中心的根基也是零．

4．在任意环中，任意幂零左理想子环能够嵌入幂零理想子环．

5. 假如 L 是环 R 的极小左理想子环. 试证 $L^2=0$ 或 $L=Re$, 这里 e 是幂等元.

§7.3 半单纯环

有了上面两节，我们就容易把魏特邦定理推广，这节我们讨论半单纯环的构造.

下面先讨论半单纯环的左理想子环及理想子环. 我们知道，假如 e 是环 R 中任意元，那末 Re 是 R 的左理想子环. 当 R 是半单纯环时，它的逆也基本成立，即

定理 1 半单纯环 R 的任意非零左理想子环 L 含有幂等元 e, 并且 $L=Re$.

证明 首先因为 R 的根基是零，所以 L 不是幂零，由 §7.2 定理 2, L 含有幂等元 e.

再 L 中所有满足 $xe=0$ 的元 x 形成 R 的左理想子环，我们用 L_e 表示. 因为 L 中幂等元可能不只一个，因此所有这样的左理想子环也可能不只一个. 但 R 满足极小条件，所以所有这样的左理想子环集合有极小左理想子环. 我们假定这极小理想子环是 L_e, 也就是说，上面的幂等元 e 我们是如此选择的，假如 $L_e\neq 0$, 那末它含有幂等元 e_1, 显然 $e_1e=0$. 命 $e'=e-ee_1+e_1$, 由计算我们容易得知，$e'e'=e'$, $e'e=e\neq 0$, 所以 $e'\neq 0$, 因此 e' 是幂等元. 于是我们有左理想子环 $L_{e'}$. 再因为 $e'e=e$, $e_1e'=e_1\neq 0$, 所以 $L_{e'}\subset L_e$, 这与 L_e 是极小的假设矛盾. 于是 $L_e=0$.

假定 x 是 L 中任意元，因为 $(x-xe)e=0$, 所以 $x-xe\in L_e$. 因此 $x=xe$. 于是 $L=Le$, 即 e 是 L 的右单位元，又因为 $Le\subseteq Re\subseteq L$, 所以 $L=Re$. 因此定理成立.

定理 2 半单纯环 R 中理想子环 $N=Re=eR$, 这里 e 是 N 的

唯一单位元.

证明 因为 N 也是 R 的左理想子环，所以 $N=Re$. 再 N 中所有满足 $ex=0$ 的元 x 形成 R 的右理想子环 M. 显然 $Me=M$, $eM=0$. 于是 $M^2=MeM=0$, 因此 M 是 R 的幂零右理想子环. 但 R 的根基是零，所以 $M=0$. 于是对于 N 中任意元 x, 由 $e(x-ex)=0$, 我们就有 $x-ex=0$, 所以 $N=eN=eR$. 因此 $N=Re=eR$, e 是 N 的单位元. 因为单位元是唯一的，所以定理成立.

因为环自身也是理想子环，所以半单纯环有单位元.

假如 e 是半单纯环 R 的幂等元，如果 e 在 R 的中心，那末 e 是 R 的理想子环 $N=Re=eR$ 的单位元. 反过来，假如 e 是 R 的理想子环 $Re=eR$ 的单位元，如果 x 是 R 中任意元，因为 $ex=ex\cdot e=e\cdot xe=xe$, 所以 e 在 R 的中心. 这就是说，R 的幂等元是它的理想子环的单位元的必要充分条件是它在 R 的中心.

定理 3 半单纯环的理想子环是半单纯环.

证明 假定 L 是半单纯环 R 中理想子环 $N=Re=eR$ 的左理想子环，因为 $L\subseteq N$, 所以 $L=eL$. 因此 $RL=ReL\subseteq NL\subseteq L$, 所以 L 也是 R 的左理想子环. 因为 R 满足极小条件，所以 N 也满足极小条件. 又因为 R 中没有非零的幂零左理想子环，所以 N 也没有非零的幂零左理想子环. 因此 N 的根基是零，于是定理成立.

定理 4 假定 $N=Re=eR$ 是半单纯环 R 的理想子环，那末 N 是 R 的直和因子，即

$$R=N+N',$$

这里 N' 是 R 的理想子环，并且由 N 唯一决定.

证明 假定 1 是 R 的单位元，r 是 R 中任意元，因为

$$r=re+r(1-e),$$

所以 $R=(N,\ N')$, 这里 $N'=R(1-e)$. 但

$$N'R=R(1-e)R=R\cdot R(1-e)=R(1-e),$$

所以 N' 是 R 的理想子环. 又因为 $Ne=N, N'e=0$, 所以 $N\cap N'=0$. 于是 R 是理想子环 N, N' 的直和, 即 $R=N+N'$.

再假定 $R=N+N''$, a 是 N'' 中任意元,

$$a=b+c,\quad b\in N,\quad c\in N',$$

因为 N'' 是 R 的理想子环, 所以 $ae\in N''$, 又因为 $ae=be+ce=be=b$, 所以 $b=0$, 因此 $a=c$. 于是 $N''\subseteq N'$. 同样我们有 $N'\subseteq N''$, 所以 $N'=N''$, 这就是说, N' 是由 N 唯一决定的. 于是定理成立.

现在我们来讨论半单纯环的构造.

我们知道, 一个环如果除自身及零理想子环外没有其他理想子环, 就叫做单纯环. 环 R 的理想子环如果又是单纯环, 就叫做 R 的**单纯理想子环**. 下面是半单纯环的构造定理, 这定理又叫**魏特邦 阿丁第一构造定理**.

定理 5 半单纯环 R 只有有穷个单纯理想子环, R 是它的所有单纯理想子环的直和, 并且 R 的任意理想子环是包含在它里面的 R 的所有单纯理想子环的直和.

证明 因为 R 的理想子环 N 仍然是半单纯环, 并且 N 的理想子环又是 R 的理想子环, 因此只要证明定理的前半段, 后半段就是显然的了.

根据极小条件我们容易得知, R 中所有非零理想子环集合的极小理想子环是 R 的单纯理想子环, 这就是说, R 含有单纯理想子环. 假定 N_1 是 R 的单纯理想子环, 由定理 4, 我们有

$$R=N_1+N_1',$$

这里 N_1' 是 R 的理想子环. 如果 $N_1'\neq 0$ 又不是单纯理想子环, 那末 N_1' 含有 R 的单纯理想子环 N_2, 于是我们有 $N_1'=N_2+N_2'$, 因此

$$R=N_1+N_2+N_2'.$$

如果 $N_2'\neq 0$ 又不是 R 的单纯理想子环, 我们又可继续分解. 因为

R 满足极小条件，所以 R 的理想子环列

$$R \supset N_1' \supset N_2' \supset \cdots$$

只能有有穷项，因此有整数 n 存在，使 $N_n'=0$. 于是

$$R=N_1+N_2+\cdots+N_n.$$

这就是说，R 是 n 个单纯理想子环的直和.

假如我们能够证明 R 的任意有穷个单纯理想子环的和都是直和，那末 R 就只有 n 个单纯理想子环，因此 R 就是它的所有单纯理想子环的直和，定理就告成立.

假定 $N_i=Re_i=e_iR$, $i=1, \cdots, m$, 是 R 的 m 个单纯理想子环，因为 $N_i \cap N_j$, $i \neq j$, 是 N 的理想子环，所以 $N_i \cap N_j=0$, 因此 $N_iN_j=0$. 于是 $e_iN_j=0$.

如果 $$a_1+\cdots+a_m=0, \quad a_i \in N_i,$$

那末 $$e_ia_i=a_i=0.$$

因此 $(N_1, \cdots, N_m)$ 中任意元能够一意地表为 $N_1, \cdots, N_m$ 中元的和，所以 $(N_1, \cdots, N_m)=N_1+\cdots+N_m$, 因此定理成立.

于是半单纯环的构造由它的所有单纯理想子环的构造一意决定，因此半单纯环的构造问题可以归结为单纯环的构造问题了. 下节我们还要详细讨论单纯环的构造.

假如半单纯环 R 是它的 n 个单纯理想子环的直和，那末 R 中互异的理想子环就只有 2^n 个.

由 §3.6 定理 3，我们得知非幂零的可换单纯环是体，因此由定理 5 我们即得下面的德狄亭得(I. W. R.Dedekind, 1831~1916) 定理.

定理 6 元数大于 1 的可换半单纯环是有穷个可换体的直和.

假定 $R \neq 0$ 是满足极小条件的单纯环，N 是它的根基，因为

R^2 是 R 的理想子环，所以 $R^2=R$ 或 $R^2=0$. 又因为 N 是 R 的理想子环，并且是幂零，所以当 $R^2=R$ 时，$N=0$; 当 $R^2=0$ 时，$N=R$. 这就是说当 $R^2=R$ 时，R 是半单纯环；当 $R^2=0$ 时 R 是根基环，即非幂零单纯环是半单纯环，幂零单纯环是根基环.

下面是定理 5 的逆.

定理 7 假定 R 是满足极小条件的单纯环 $R_1,\cdots,R_n(R_i^2\neq 0)$ 的直和，即 $R=R_1+\cdots+R_n$, 那末 R 是半单纯环.

证明 因为 $R_i^2\neq 0$. 所以 R_i 又是半单纯环，因此它有单位元，于是 R 也有单位元. 根据假设 R_i 满足极小条件，由 §7.1 定理 1 我们得知，R 也满足极小条件.

再假定 L 是 R 的幂零左理想子环，由 §5.4 定理 5 我们有

$$L=L_1+\cdots+L_n, L_i=L\cap R_i,$$

因此 L_i 是 R_i 的幂零左理想子环，但 R_i 是半单纯环，所以 $L_i=0$. 于是 $L=0$, 这就是说 R 的根基是零. 于是 R 是半单纯环，因此定理得证.

下面是单纯环与定理 4 类似的性质.

假如把定理 4 中 R 改为单纯环、N 改为 R 的左理想子环，定理仍然成立，这时 N' 是 R 的左理想子环. 但不一定是由 N 唯一决定的. 再根据定理 4 的证明我们即得

定理 8 非幂零单纯环是有穷个极小左理想子环的直和.

要注意的是，半单纯环分解为单纯理想子环的直和是唯一的，单纯环分解为极小左理想子环的直和不是唯一的. 但它的直和因子的个数是一致的. 这是因为，假如把 R 看成 R 空间，那末这时它的直和因子的个数就是它的维数，因此由 R 唯一确定. 譬如全矩阵环 Q_2 可以分解为 $Q_2E_1+Q_2E_2$, 也可以分解为 $Q_2E_1+Q_2E_3$, 即

$$Q_2=Q_2E_1+Q_2E_2,\quad Q_2=Q_2E_1+Q_2E_3,$$

这里 $E_1=\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}$, $E_2=\begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}$, $E_3=\begin{pmatrix}2 & 2\\ -1 & -1\end{pmatrix}$.

定理 9 非幂零单纯环的极小左理想子环相互同构.

证明 假定 L_1, L_2 是单纯环 R 的极小左理想子环, 如果 $L_1L_2=0$, 由 $L_2=RL_2$, 我们就有 $L_1RL_2=0$, 因此 $L_1RL_2R=0$. 但 L_1R, L_2R 都是 R 的非零理想子环, 而 R 是单纯环, 所以 $L_1R=R$, $L_2R=R$. 于是 $R^2=0$, 这与我们的假设不合, 因此 $L_1L_2\neq 0$. 于是在 L_2 中有元 a 使 $L_1a\neq 0$, 但 $L_1a\subseteq L_2$ 而 L_2 是极小左理想子环, 所以 $L_2=L_1a$. 显然 $x\to xa$ 是 L_1 射到 L_2 上的同态(看成 R 空间), 因为 L_2 是极小左理想子环, 所以这同态又是同构. 于是 $L_1\cong L_2$, 因此定理成立.

定理 10 半单纯环的极小左理想子环如果包含在同一单纯理想子环中, 它们就同构; 如果不包含在同一单纯理想子环中, 它们就不同构.

证明 假定 L_1, L_2 是半单纯环 R 的极小左理想子环, 如果 L_1, L_2 同在 R 的一个单纯理想子环中, 由上面定理 9, $L_1\cong L_2$. 如果 L_1, L_2 分别在不同的单纯理想子环 N_1, N_2 中, 因为 N_1, N_2 是 R 的直和因子, 所以 $N_1N_2=0$. 命 e_1 是 N_1 的单位元, $e_1L_1=L_1$, $e_1L_2=0$. 所以 L_1, L_2 看成 R 空间时不同构, 因此定理成立.

要注意的是, 上面的同构都是看成 R 空间时的同构, 而不是环的同构.

定理 11 假定 L 是任意环 R 的左理想子环, 那末 R 中所有与 L 同态(看成 R 空间)的左理想子环的和是 R 的理想子环.

证明 R 中所有与 L 同态的左理想子环的和 N 显然是 R 的左理想子环. 假定 a 是 R 中任意元, L' 是 R 中与 L 同态的任意左理想子环, 那末 $L'a$ 又是 R 的左理想子环. 假如 $x\to x'$ 是 L 与 L' 的同态, 那末 $x\to x'a$ 就是 L 与 $L'a$ 的同态, 所以 $L\sim L'a$, 于是

$L'a \in N$，因此 $NR \subseteq N$，这就是说 N 是 R 的理想子环，所以定理得证.

于是我们得知，半单纯环 R 假如先分解为单纯理想子环的直和，再把各个单纯理想子环分解为极小左理想子环的和，我们就得到 R 分解为极小左理想子环的直和．假如先分解为极小左理想子环的直和，再把其中所有相互同构的极小左理想子环合并，我们就得到 R 分解为单纯理想子环的直和.

习 题 7.3

1. 半单纯环的中心是可换体的直和.

2. 假如 e_1, e_2 是环 R 的幂等元，如果 $e_1e_2=e_2e_1=0$，那末 e_1, e_2 叫做**正交幂等元**．一个幂等元，如果不能写成两个正交幂等元的和，就叫做**本原幂等元**．试证半单纯环 R 的左理想子环 $L=Re$ 是极小的必要充分条件为：e 是本原幂等元.

3. 试证 K_nE_{ii} 是全矩阵环 K_n 的极小左理想子环，并且 $K_n=K_nE_{11}+\cdots+K_nE_{nn}$，这里 K 是体.

4. 假如环 R 有单位元，并且是有穷个极小左理想子环的直和，那末 R 是半单纯环.

§7.4 单 纯 环

上节讨论了半单纯环的构造，这节讨论满足极小条件的单纯环的构造.

我们知道，假如单纯环 $R\neq0$，那末当 $R^2\neq0$ 时，R 是半单纯环，当 $R^2=0$ 时，R 是根基环，这时 R 中任意两元的乘积都是零．同 §3.6 定理 1 一样，R 的元数是质数．于是我们有

定理 1 单纯环 R 如果 $R^2=0$，那末它是根基环，它的元数是质数.

下面是非幂零单纯环的构造定理，这定理又叫做**魏特邦-阿丁第二构造定理**，这节主要是证明这定理.

定理 2 单纯环 R 如果 $R^2 \neq 0$，即 R 是非幂零单纯环，那末 R 与全矩阵环 K_n 同构，并且整数 n 及体 K（除同构外）由 R 一意决定，这 K 叫做 R **所属体**.

这定理就是说 R 中元可以用矩阵来表示. 在线代数中我们曾证明，向量空间的线性变换可以用矩阵表示. 我们这里与它类似，证明方法基本上一样. 我们首先要求建立一个体 K 的有穷维向量空间，R 中元是这向量空间的线性变换，再求出与 R 中元对应的矩阵，然后根据同构定义，证明 R 与这些矩阵形成的全矩阵环同构，于是证明完毕. 下面我们就是根据这个步骤来逐步完成定理的证明.

首先我们来建立体 K，关于这我们有

定理 3 假定环 R（不要求满足极小条件）不含非零的幂零左理想子环，e 是 R 的幂等元，那末左理想子环 $L = Re$ 是极小左理想子环的必要充分条件是：eRe 是体.

证明 假定 $L = Re$ 是 R 的极小左理想子环，我们来证明 eRe 是体. 容易知道 eRe 是环，这是因为，形状象 ere，$r \in R$，的元的和、差、积仍然是这样形状的元. 又因为 e 是幂等元，所以 e 是 eRe 的单位元. 再假定 $ere \neq 0$，那末 $Rere$ 是 L 中 R 的非零左理想子环，因为 L 是极小左理想子环，所以 $Rere = Re$，于是 $uere = e$ 中 u 就是 ere 的逆元，这就是说，eRe 中任意非零元都有逆元，因此 eRe 成体.

反过来，假如 eRe 是体，我们来证明 $L = Re$ 是极小左理想子环. 假定 $L' \neq 0$ 是 L 中 R 的左理想子环，如果 $eL' = 0$，那末 $L'L' \subseteq LL' = 0$，这与 R 中不含非零的幂零左理想子环的假设不合，因此 $eL' \neq 0$. 于是 eL' 是体 eRe 的非零左理想子环，所以 $eL' = eRe$. 因

此 $e\in eL'\subseteq L'$, 所以

$$L=Re\subseteq RL'\subseteq L',$$

于是 $L=L'$, 这就是说, L 是 R 的极小左理想子环, 因此定理成立.

假如把上定理中左理想子环换成右理想子环, 显然定理仍然成立. 这就是说, 假如环 R 不含非零的幂零右理想子环, 那末 $M=eR$ 是 R 的极小右理想子环的必要充分条件是: eRe 成体. 因此, 假如环 R 不含非零的幂零左理想子环, 也不含非零的幂零右理想子环, 如果 Re 是 R 的极小左理想子环, 那末 eR 就是 R 的极小右理想子环.

这样, 我们得到 $K=eRe$, 再我们来建立 K 的有穷维向量空间.

假定 R 是单纯环, $L=Re$ 是 R 的极小左理想子环, $K=eRe$. 命 $V=eR$, 因为

$$KV=eRe\cdot eR\subseteq eR=V,$$

所以 V 是体 K 空间. 下面我们来讨论 V 的维数.

假定 $u_1, \cdots, u_n$ 是 V 中关于 K 线性无关的元, 因为 $eu_i=u_i\neq 0$, 所以 $Lu_i\neq 0$. 又因为 L, Lu_i 看成 R 空间时是同构, 所以 Lu_i 是 R 的极小左理想子环. 假如我们能够证明 $Lu_1, \cdots, Lu_n$ 的和 $(Lu_1, \cdots, Lu_n)$ 是直和, 那末 V 关于 K 的维数就不大于 R 的长. 反过来, 假如 V 关于 K 的维数是 n, 命 $V=Ku_1+\cdots+Ku_n$, 因为 $LV=ReR$ 是 R 的理想子环, 所以 $R=LV$. 又因为 $LK=Re\cdot eRe\subseteq L$, 而 LK 是 R 的左理想子环, 所以 $LK=L$. 于是 $R=(Lu_1, \cdots, Lu_n)$, 这就是说, R 的长不大于 V 的维数. 因此, 只要我们能够证明 $(Lu_1, \cdots, Lu_n)=Lu_1+\cdots+Lu_n$, 那末 V 关于 K 的维数就是 R 的长了.

要证明 $(Lu_1, \cdots, Lu_n)$ 是直和, 只要证明

$$a_1u_1+\cdots+a_nu_n=0, \quad a_i\in L$$

时，$a_iu_i=0$，$i=1$，…，n. 我们用反证法来证明. 假定 a_iu_i 不完全都是零，譬如 $a_1u_1\neq 0$，那末 $a_1u_1\in(Lu_2, \cdots, Lu_n)$，因此左理想子环 $(Lu_2, \cdots, Lu_n)$ 与极小左理想子环 Lu_1 的交集异于零，于是

$$Lu_1\subseteq(Lu_2, \cdots, Lu_n).$$

因为 $u_1\in Lu_1$，所以我们有

$$u_1+a_2'u_2+\cdots+a_n'u_n=0, \quad a_i'\in L,$$

即

$$eu_1+ea_2'u_2+\cdots+ea_n'u_n=0.$$

但 e, ea_i' 都是 K 中元而 $e\neq 0$，这与 u_1，…，u_n 关于 K 线性无关的假设不合，所以 Lu_1，…，Lu_n 的和是直和.

于是我们有

定理 4 假定 R 是非幂零单纯环，它的长是 n，$L=Re$ 是 R 的极小左理想子环，$K=eRe$，那末 $V=eR$ 是 n 维 K 向量空间.

由上面的证明我们还知道，假如 u_1，…，u_n 是 V 关于 K 的底，即 $V=Ku_1+\cdots+Ku_n$，那末 R 就是极小左理想子环 Lu_1，…，Lu_n 的直和，即 $R=Lu_1+\cdots+Lu_n$.

有了 K 向量空间 V，就容易求得与 R 中元对应的矩阵了.

假定 $V=Ku_1+\cdots+Ku_n$，因为 V 是 R 的右理想子环，所以对于 R 中元 a，我们有

$$u_ia=a_{i1}u_1+\cdots+a_{in}u_n, \quad a_{ij}\in K,$$

因此

$$\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}a=\begin{pmatrix}u_1a\\ \vdots\\ u_na\end{pmatrix}=A_a\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}, \quad A_a=(a_{ij}).$$

即对于元 a 我们有矩阵 A_a. 同样对于 R 中元 b，我们有

$$\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}b=A_b\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}, \quad A_b=(b_{ij}).$$

于是

$$\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}(a+b)=A_{a+b}\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}, \quad \begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}ab=A_{ab}\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}.$$

但
$$\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}(a+b)=\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}a+\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}b=A_a\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}+A_b\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}$$
$$=(A_a+A_b)\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix},$$
$$\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}ab=\left\{\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}a\right\}b=A_a\left\{\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}b\right\}=A_aA_b\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}.$$

因此
$$A_{a+b}\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}=(A_a+A_b)\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix},\quad A_{ab}\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}=A_aA_b\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}.$$

因为 $u_1, \cdots, u_n$ 关于 K 线性无关，所以
$$A_{a+b}=A_a+A_b,\quad A_{ab}=A_a\cdot A_b.$$
于是映射 $a\to A_a$ 是 R 射到 K_n 内的同态. 根据下面定理 5，这同态是 R 射到 K_n 上的，并且又是一对一的. 所以这同态是同构，这就是说 R 与 K_n 同构.

定理 5 假定 $v_1, \cdots, v_n$ 是非幂零单纯环 R 的极小右理想子环 $V=eR=Ku_1+\cdots+Ku_n$ 中任意 n 个元，那末 R 中有一且只有一个满足
$$v_i=u_ir,\quad i=1, \cdots, n,$$
的元 r.

证明 我们先证明 r 的唯一性. 假定 $u_ir=u_ir'$, $i=1, \cdots, n$, 那末 $u_i(r-r')=0$, 但 R 中所有适合
$$u_ix=0,\quad i=1, \cdots, n,$$
也就是使 $Vx=0$ 的元 x 形成 R 的右理想子环 N, 因为 V 是 R 的右理想子环，所以 N 又是 R 的左理想子环，于是 N 是 R 的理想子环. 因为 $VR=V\neq 0$, 所以 $N=0$, 这就是说，只有 $x=0$ 适合上式，因此 $r=r'$.

再来证明 r 的存在性. 我们容易知道，假如能够找到适合

$$u_i r_i = v_i,\quad u_j r_i = 0,\quad j \neq i,\ i = 1, \cdots, n,$$

的元 r_i，那末 $r_1 + \cdots + r_n$ 就是所求的 r. 下面我们来讨论如何找这样的 r_i.

我们先求 r_1. 假定 $L' = Lu_2 + \cdots + Lu_n$，因为 L' 是 R 的左理想子环，所以我们把它写成 $L' = Re'$，这里 e' 是幂等元，并且 $e' \neq 1$. 再因为

$$L'(1 - e') = Re'(1 - e') = R(e' - e') = 0,$$

所以
$$u_i(1 - e') = 0,\quad i = 2, \cdots, n.$$

但 $R = Lu_1 + \cdots + Lu_n$. 如果 $u_1(1 - e') = 0$，那末 $R(1 - e') = 0$，于是 $1 \cdot (1 - e') = 1 - e' = 0$，这与 $e' \neq 1$ 的假设不合，所以 $u_1(1 - e') \neq 0$. 于是 $u_1(1 - e')R$ 是 R 的非零右理想子环. 因为 $u_1(1 - e')R \subseteq V$，而 V 是 R 的极小右理想子环，所以 $u_1(1 - e')R = V$，因此在 R 中有满足

$$u_1(1 - e')r'_1 = v_1$$

的元 r'_1，显然这时

$$u_i(1 - e')r'_1 = 0,\quad i = 2, \cdots, n,$$

所以 $(1 - e')r'_1$ 就是所求的 r_1，即 $r_1 = (1 - e')r'_1$. 同样我们可以求得 $r_2, \cdots, r_n$，这就证明了 $r_1, \cdots, r_n$ 的存在性. 于是定理成立.

定理 2 中尚未证明的只是一意性. 也就是说，假如单纯环 $R \simeq K_n$，那末整数 n 由 R 一意决定，体 K 除同构外也由 R 一意决定. 最后我们解答这问题.

首先我们知道，全矩阵环 K_n 可以写成 n 个极小左理想子环的直和，所以 K_n 的长是 n，因此 n 就是 R 的长，所以 n 由 R 一意决定.

再因为 $R \simeq K_n$，命 e 是 R 中与 K_n 中元 $\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$ 对应的元，即

$$e\to\begin{pmatrix}1 & \\ & 0\end{pmatrix},$$

那末 e 是幂等元,并且对于 R 中任意元 r,

$$ere\to\begin{pmatrix}1 & \\ & 0\end{pmatrix}\begin{pmatrix}k_{11} & \cdots & k_{1n}\\ \cdots & \cdots & \cdots\\ k_{n1} & \cdots & k_{nn}\end{pmatrix}\begin{pmatrix}1 & \\ & 0\end{pmatrix}=\begin{pmatrix}k_{11} & \\ & 0\end{pmatrix},$$

因为这映射是 R 与 K_n 的同构,所以 $eRe\cong K$. 根据下定理, eRe 与 R 的极小左理想子环 $L=Re$ 的自同态环逆同构,但 R 的极小左理想子环相互同构,因此它们的自同态环也彼此同构,这样,eRe 就是由 R 一意决定的体了. 所以 K 除同构外由 R 一意决定. 于是定理 2 中唯一性就完全得证.

定理 6 假定 $L=Re$ 是环 R 的极小左理想子环,那末 L 的自同态环 S 是 eRe 的逆环.

证明 假定 σ 是 $L=Le$ 的自同态,$\sigma(e)=ae$, $a\in L$, 那末对于 L 中任意元 re, $r\in L$,

$$\sigma(re)=r\sigma(e)=rae,$$

因此 re 的象由 e 的象 ae 决定,所以我们又把 σ 写成 σ_a. 因为 $a\in L$, 所以 $a=ae$, 又因为

$$ae=\sigma(e)=\sigma(ee)=e\sigma(e)=eae,$$

所以 $a=eae$, 即 $a\in eRe$. 这就是说,L 的任意同态 σ_a 由 eRe 中元 a 决定. 反过来,假如 a 是 eRe 中任意元,显然映射

$$e\to ae,\quad re\to rae,\quad r\in L,$$

就是 L 的自同态 σ_a. 因为 e 是 L 的右单位元, 所以当 $a\neq b$ 时 $ae\neq be$,因此 $\sigma_a\neq\sigma_b$.

命 $a\to\sigma_a$, 那末这映射是 eRe 射到 L 的自同态环 S 上的一对一的映射. 再我们容易得知

$$(\sigma_a+\sigma_b)e=\sigma_a(e)+\sigma_b(e)=(a+b)e=\sigma_{a+b}(e),$$

$$\sigma_a\sigma_b(e)=\sigma_a\{\sigma_b(e)\}=\sigma_a(be)=b\sigma_a(e)=bae=\sigma_{ba}(e),$$

所以 $$\sigma_a+\sigma_b=\sigma_{a+b},\quad \sigma_a\sigma_b=\sigma_{ba}.$$

于是 $a\to\sigma_a$ 是 eRe 射到 S 上的逆同构，因此 eRe 是 S 的逆环．所以定理成立．

于是上面定理 2 完全得证．

由上面的证明我们得知 R 包含它的所属体 $K=eRe$．又假如 a 是 R 的中心 C 中任意元．因为 $ae=ae^2=eae\in K$，所以由

$$u_ia=eu_ia=eau_i=aeu_i,$$

我们就得到

$$A_a=\begin{pmatrix}ae & & \\ & \ddots & \\ & & ae\end{pmatrix}=a\begin{pmatrix}e & & \\ & \ddots & \\ & & e\end{pmatrix}=aE,\quad E=\begin{pmatrix}e & & \\ & \ddots & \\ & & e\end{pmatrix}.$$

这就是说，上面的同构把 R 的中心 C 中元 a 变为 K_n 中元 aE，因为同构把中心变为中心，所以 K_n 的中心是 CE．这结果也可由§3.1 习题 8 推得．

下面是定理 2 的逆．

定理 7 假定 K 是体，那末全矩阵环 K_n 是非幂零的单纯环．

证明 由§7.1 定理 3，K_n 满足极小条件．

再假定 N 是 K_n 中任意非零的理想子环，a 是 N 中非零元，E_{ij} 是 n 阶矩阵，其 i 行 j 列是 K 的单位元 1，其余都是零元 0，于是

$$a=\sum a_{ij}E_{ij},\quad a_{ij}\in K,$$

因为 $a\neq0$，所以 a_{ij} 不完全是 0．假定 $a_{rs}\neq0$，根据

$$\begin{aligned}E_{ij}E_{kl}&=0, &&\text{当 } j\neq k;\\ &=E_{il}, &&\text{当 } j=k,\end{aligned}$$

对于 K 中任意元 b，我们有

$$ba_{rs}^{-1}E_{ir}aE_{sj}=bE_{ij}\in N,$$

因此 $K_n\subseteq N$，所以 $N=K_n$，这就是说，K_n 中任意非零的理想子环

只有单位理想子环，所以 K_n 是单纯环. 于是定理得证.

习 题 7.4

1. 试证有穷非幂零单纯环是它的中心上的全矩阵环.
2. 试证 n 维 K 向量空间的自同态环与全矩阵环同构.
3. 半单纯环是单纯环的必要充分条件是它的中心是体.
4. 假如 e 是单纯环 R 的幂等元，试证 eRe 是体的必要充分条件是 e 是本原幂等元.

§7.5 贾柯勃逊根基

前面我们讨论了满足极小条件的环的构造，此后三节讨论一般环的构造. 我们先由贾柯勃逊根基开始.

§7.2 中满足极小条件的环的根基是用幂零元、幂零左理想子环建立的. 1942 年皮里斯(S. Perlis)把幂零元的概念推广，在一般环中引进左拟正则元[9]. 1945 年贾柯勃逊用左拟正则元把前面的根基概念推广，创造了一般环的根基，建立了一般环的构造理论[5].

假定 a 是有单位元 1 的环中一元，如果 $1+a$ 有左逆，我们把这左逆写成 $1+a'$，那末 $(1+a')(1+a)=1$，因此

$$a+a'+a'a=0. \tag{1}$$

反过来，假如 a 是环中一元，如果有满足(1)的 a' 存在，那末 $1+a'$ 是 $1+a$ 的左逆元. 在一般环 R 中我们根据(1)引进一个新的结合法，对于 R 中两元 a, a'，我们规定

$$a\circ a'=a+a'+a'a,$$

这结合法$\circ$叫做 R 的拟乘法. 显然，拟乘法满足结合律，并且 R 的零元 0 是它的单位元，即

$$(a\circ b)\circ c=a\circ(b\circ c),\quad a\circ 0=0\circ a=a.$$

当 $a\circ a'=0$ 时我们叫 a' 是 a 的**右拟逆元**，a 是 a' 的**左拟逆元**，这时我们又说 a 是 R 的**左拟正则元**，a' 是 R 的**右拟正则元**．R 中 a，如果是左拟正则元同时又是右拟正则元，那末 a 就叫做 R 的**拟正则元**．

假如 a 是 R 的拟正则元，那末 a 的左拟逆元也是 a 的右拟逆元，因此是 a 的**拟逆元**．这是因为 $\circ$ 适合结合律，由 $a\circ a'=0, a''\circ a=0$，我们就有

$$a''=a''\circ 0=a''\circ(a\circ a')=(a''\circ a)\circ a'=0\circ a'=a'.$$

即 $a\circ a'=a'\circ a=0$．于是一个拟正则元的拟逆元是唯一的．

显然环 R 的零元是 R 的拟正则元．R 的幂零元也是 R 的拟正则元，这是因为，假如 $a^n=0$．命 $a'=-a+a^2-a^3+\cdots+(-1)^{n-1}a^{n-1}$．我们容易验证 $a\circ a'=a'\circ a=(-1)^{n-1}a^n=0$．但拟正则元一般不是幂零元．譬如在由所有有理数 $\frac{n}{m}$，这里 m 是奇数，n 是任意整数，形成的环中，没有非零的幂零元，但任意形状象 $\frac{2n}{m}$ 的元都是拟正则元，这是因为

$$\frac{2n}{m}+\frac{-2n}{2n+m}+\frac{2n(-2n)}{m(2n+m)}=0.$$

当环 R 有单位元 1 时，元 r' 是 r 的左拟逆元的必要充分条件是：$1+r'$ 是 $1+r$ 的左逆元．因此整数环只有零元是左拟正则元．

定理　环 R 中元 r 是左拟正则元的必要充分条件是：

$$\{x+xr\mid x\in R\}=R.$$

证明　因为所有形状象 $x+xr$，$x\in R$，的元形成 R 的左理想子环 $\{x+xr\}$．假如 r 是左拟正则元，那末 $-r=r'+r'r\in\{x+xr\}$，因此 $xr\in\{x+xr\}$．于是 $x\in\{x+xr\}$，所以 $\{x+xr\}=R$．反过来，假如 $\{x+xr\}=R$，那末 $-r=r'+r'r$，即 $r+r'+r'r=0$，所

以 r 是左拟正则元. 于是定理成立.

一般,一个左拟正则元不一定又是右拟正则元,但有时却能如此.

假如 L 是环 R 的左理想子环, 如果其中任意元 a 是 R 的左拟正则元,那末 a 又是 R 的右拟正则元,因此 a 是 R 的拟正则元. 这是因为, 由 $a\circ a'=0$, 得知 a' 是 R 的右拟正则元, 但 $a'=-a-a'a\in L$, 所以 a' 又是 R 的左拟正则元, 因此我们有 $a\circ a'=a'\circ a=0$, 即 a 是 R 的拟正则元.

同样,在环 R 的右理想子环中任意元如果都是 R 的右拟正则元,那末它们也都是 R 的拟正则元.

下面的定义与幂零左理想子环类似.

定义 1 环 R 的左(右)理想子环, 其中任意元都是 R 的左(右)拟正则元时, 叫做 R 的**拟正则左(右)理想子环**. R 的理想子环, 其中任意元都是 R 的拟正则元时, 叫做 R 的**拟正则理想子环**.

于是拟正则左或右理想子环中元都是拟正则元, 拟正则左或右理想子环如果又是理想子环,那末它就是拟正则理想子环.

因为幂零元是拟正则元. 所以在一般环中幂零元左理想子环是拟正则左理想子环. 在满足极小条件的环中,反过来也成立,即

定理 1 假定 L 是环 R 的拟正则左理想子环,如果 R 满足极小条件,那末 L 是幂零左理想子环.

证明 假定 $L\supset L^2\supset L^3\supset\cdots$,根据极小条件,我们有某正整数 k 存在, 使 $L^k=L^{k+1}$. 命 $P=L^k$, 下面我们用反证法来证明 $P=0$.

假如 $P\neq 0$, 我们命 N 是 R 中满足下列条件的极小左理想子环,

$$PN\neq 0.$$

显然 N 是存在的，因为 P 自身就满足这条件．于是 N 中有元 a 使 $Pa\neq 0$．因为 $P^2=P$，所以 $P(Pa)=P^2a=Pa\neq 0$，但 $Pa\subseteq N$，而 N 是极小左理想子环．所以 $Pa=N$．于是 P 中有元 x 使 $xa=a$，因为 $x\in P$，所以 x 是 R 的左拟正则元，即 $-x+x'-x'x=0$，因此

$$a=a+(-x+x'-x'x)a=a-xa+x'(a-xa)=0,$$

这与 $Pa\neq 0$ 的假设矛盾．所以 $P=0$，即 $L^k=0$，这就是说，L 是幂零左理想子环．所以定理成立．

现在我们用拟正则左理想子环代替 §7.2 中幂零左理想子环来建立一般环的根基．

下面是与 §7.2 中类似的定理．

定理 2　假定 L_1，L_2 是环 R 的拟正则左理想子环，那末它们的和 (L_1, L_2) 也是 R 的拟正则左理想子环．

证明　假定 $a\in L_1$，$b\in L_2$．那末我们有

$$a+a'+a'a=0,\quad b+b'+b'a=0.$$

又因为 $b+a'b\in L_2$，所以我们又有

$$b+a'b+c+c(b+a'b)=0,$$

于是

$$\begin{aligned}&a+b+(a'+c+ca')+(a'+c+ca')(a+b)\\&=(a+a'+a'a)+\{b+a'b+c+c(b+a'b)\}\\&\quad+c(a+a'+a'a)=0,\end{aligned}$$

所以 $a+b$ 是 R 的左拟正则元，因此 (L_1, L_2) 是 R 的拟正则左理想子环，于是定理成立．

定理 3　环 R 中所有拟正则左理想子环的和是 R 的拟正则理想子环．叫做 R 的**贾柯勃逊根基**或简称 R 的**根基**，用 $J(R)$ 或 J 表示．

有时为了避免混淆，§7.2 中根据幂零左理想子环给出的根基又叫做**幂零根基**．

证明　因为 J 中任意元是 R 中某有穷个拟正则左理想子环中元的和，由上定理，它是 R 的左拟正则元，所以 J 是 R 的拟正则左理想子环.

下面我们来证明 J 是 R 的理想子环. 假定 a 是 J 中任意元，r 是 R 中任意元，如果我们能够证明 $ar\in J$，那末 J 又是 R 的右理想子环，因此 J 就是 R 的理想子环了.

因为 J 是 R 的左理想子环，所以 $ra\in J$，即 ra 是 R 的左拟正则元，因此我们有

$$ra+b+bra=0,$$

于是

$$\begin{aligned} &ar+(-ar-abr)+(-ar-abr)ar \\ &=-a(b+ra+bra)r=0, \end{aligned}$$

所以 ar 是 R 的左拟正则元. 再因为由 ar 生成的 R 的左理想子环 L 中任意元可以写成 $sar+nar=(sa+na)r$，这里 $s\in R$，n 是整数，同上面证明一样，它是 R 的左拟正则元，因此 L 是 R 的拟正则左理想子环. 所以 $L\subseteq J$，于是 $ar\in J$. 因此定理成立.

上面根基概念是根据 R 的拟正则左理想子环建立的. 假如我们把左理想子环换成右理想子环，引用拟正则右理想子环，我们同样可以建立根基，并且也得到同样的性质. 假如这时得出的根基用 J' 表示，那末 $J'=J$. 这是因为，J' 是 R 的理想子环，并且其中任意元是 R 的拟正则元，所以 J' 是 R 的拟正则左理想子环，因此 $J'\subseteq J$. 同样我们有 $J\subseteq J'$，所以 $J'=J$.

于是 J 既包含 R 的所有拟正则左理想子环，同时也包含 R 的所有拟正则右理想子环. 又因为 R 的幂零元左理想子环是 R 的拟正则左理想子环，R 的幂零元右理想子环是 R 的拟正则右理想子环，所以 J 又包含 R 的所有幂零元左理想子环，也包含 R 的所有幂零元右理想子环. 在可换环中，任意幂零元生成的理想子环是幂零元理想子环，因此可换环的根基包含环中所有幂零元，但它可

能还包含其他非幂零的拟正则元.

当环 R 满足极小条件时，因为这时拟正则左理想子环是幂零左理想子环，所以根基 J 是所有幂零左理想子环的和，它就是幂零根基. 这就是说，贾柯勃逊根基是幂零根基的推广.

定义 2 环 R 如果它的根基 $J=0$，那末 R 叫做**半单纯环**，如果 $J=R$，那末 R 叫做**根基环**.

为了区别，§7.2 中半单纯环有时又叫做**幂零半单纯环**，这里的半单纯环有时又叫做**贾柯勃逊半单纯环**.

定理 4 假定 J 是环 R 的根基，那末 $\bar{R}=R-J$ 是半单纯环.

证明 假定 $\bar{L}=L-J$ 是 $\bar{R}$ 中任意拟正则左理想子环，$\bar{a}$ 是 $\bar{L}$ 中任意元，那末在 $\bar{R}$ 中有元 $\bar{a}'$ 使

$$\bar{a}+\bar{a}'+\bar{a}'\bar{a}=\bar{0},$$

所以

$$a+a'+a'a\in J,$$

于是 R 中有元 u，使

$$a+a'+a'a+u+u(a+a'+a'a)=0,$$

即

$$a+(a'+u+ua')+(a'+u+ua')a=0.$$

因此 a 是 R 的左拟正则元，所以 L 是 R 的拟正则左理想子环，因此 $L\subseteq J$. 于是 $\bar{L}=\bar{0}$，这就是说，$\bar{R}$ 中任意拟正则左理想子环是零理想子环，所以 $\bar{R}$ 的根基是零，因此 $\bar{R}$ 是半单纯环. 于是定理成立.

定理 5 假定 R 是环，那末全矩阵环 R_n 的根基 $J(R_n)$ 是 R 的根基 $J(R)$ 上的全矩阵环 $(J(R))_n$，即 $J(R_n)=(J(R))_n$.

证明 我们先证明 $J(R_n)\subseteq(J(R))_n$.

假定 L_{ij} 是 $J(R_n)$ 中矩阵的第 i 行第 j 列上元的集合，显然 L_{ij} 是 R 的理想子环. 命 E_{ij} 是第 i 行第 j 列上元是 1、其余元都是零的 n 阶矩阵，那末

$$RE_{1i}J(R_n)E_{j1}R\subset J(R_n),$$

因此 $$RL_{ij}RE_{11}\subset J(R_n),$$

即 $$\begin{pmatrix} a & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}\in J(R_n),$$

这里 $$a\in RL_{ij}R.$$

于是它是左拟正则元. 因此我们有

$$\begin{pmatrix} a & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}+\begin{pmatrix} a'_{11} & \cdots & a'_{1n} \\ \cdots & \cdots & \cdots \\ a'_{n1} & \cdots & a'_{nn} \end{pmatrix}+\begin{pmatrix} a'_{11} & \cdots & a'_{1n} \\ \cdots & \cdots & \cdots \\ a'_{n1} & \cdots & a'_{nn} \end{pmatrix}\begin{pmatrix} a & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}=\begin{pmatrix} 0 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix},$$

所以 $a+a'_{11}+a'_{11}a=0$, 这就是说, $RL_{ij}R$ 中任意元是 R 的左拟正则元, 因此 $RL_{ij}R$ 是 R 的拟正则理想子环. 于是 $RL_{ij}R\subset J(R)$, 所以 $RL_{ij}RL_{ij}\subset J(R)$, 即 $(\bar{R}\bar{L}_{ij})^2=\bar{0}$, 但 $\bar{R}=R-J(R)$ 的根基是零, 所以 $\bar{L}_{ij}=0$. 因此 $L_{ij}\subset J(R)$, 这就是说, 假如 $(a_{ij})\in J(R_n)$, 那末 $a_{ij}\in J(R)$, 所以 $J(R_n)\subseteq (J(R))_n$.

再我们来证明 $(J(R))_n\subseteq J(R_n)$.

我们来考虑所有形状象

$$A_1=\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & 0 & \cdots & 0 \end{pmatrix},\quad a_{i1}\in J(R),$$

的集合 M_1, 显然 M_1 是 R_n 的左理想子环. 假定

$$A'=\begin{pmatrix} a'_{11} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix},\quad a_{11}+a'_{11}+a'_{11}a_{11}=0,$$

那末 $A_1\circ A'=\begin{pmatrix} 0 & \cdots & 0 \\ a_{21} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & 0 \end{pmatrix}$, 因此 $A_1\circ A'$ 是幂零元, 所以它也是左拟正则元. 于是有 $(A_1\circ A')\circ B=0$, $B\in R_n$, 即 $A_1\circ(A'\circ B)=0$. 这就是说, A_1 是 R_n 的左拟正则元, 所以 M_1 是 R_n 的拟正则左理想子环. 同样, 所有第 i 列是 $J(R)$ 中元, 其余元都是零的 n 阶矩阵 A_i 的集合 M_i 形成 R_n 的拟正则左理想子环. 因此 $M_1+\cdots+M_n$ 也是 R_n

的拟正则左理想子环．再因为 $(J(R))_n$ 中任意元可以分解为象 $A_1, \cdots, A_n$ 这样的 n 个矩阵的和，因此它在 $M_1+\cdots+M_n$ 中，所以 R_n 的任意左拟正则元都在 $J(R_n)$ 中，这就是说 $(J(R))_n\subseteq J(R_n)$．因此定理成立．

环的根基与它的子环的根基的关系我们还不清楚．假如子环是理想子环，我们有下面重要定理．

定理 6　假定 N 是环 R 的理想子环，那末

$$J(N)=N\cap J(R).$$

证明　假定 $a\in N\cap J(R)$，因为 $a\in J(R)$，所以对于 R 中任意元 x，得知 xa 是 R 的左拟正则元，即 R 中有元 y 使 $xa+y+yxa=0$，又因为 $a\in N$，所以 $y\in N$．于是 Na 是 N 的拟正则左理想子环．所以 $a\in J(N)$，即 $N\cap J(R)\subseteq J(N)$．

再假定 $a\in J(N)$，因为 $(Ra)^2\subseteq Na$，所以 $(Ra)^2$ 是 R 的拟正则左理想子环，因此 $(Ra)^2\subseteq J(R)$．于是 $\overline{Ra}^2=\bar{0}$，但 $\bar{R}=R-J(R)$ 是半单纯环，所以 $\overline{Ra}=\bar{0}$，即 $Ra\subseteq J(R)$，因此 $a\in J(R)$．于是 $J(N)\subseteq N\cap J(R)$．所以定理成立．

于是半单纯环的理想子环仍然是半单纯环．这与 §7.3 定理 3 是一致的．

显然，幂零元环是根基环．一个环的根基自身是根基环，即 $J(J(R))=J(R)$．有单位元的环不是根基环，因为 -1 不是拟正则元．这是因为由 $-1+a'+a'(-1)=0$，即得 $-1=0$，这显然是矛盾．

假如 R 不是根基环，那末 R 含有不是左拟正则元的元 a，因此 R 的左理想子环 $L=\{ra+r\mid r\in R\}$ 不包含 a．这是因为，如果 $a\in L$，那末 R 中有元 a'，使 $a'a+a'=-a$，即 $a+a'+a'a=0$，这与 a 不是拟左正则元的假设不合．我们来考虑 R 中所有包含 $\{ra+r\}$ 而不包含 a 的左理想子环，根据集合的包含，由冲恩引理，我们

有包含$\{ra+r\}$而不包含 a 的极大左理想子环．这左理想子环，显然也是 R 的极大理想子环，因为如果另有包含它的左理想子环，那末它就要包含 a，因此它就是 R 了．于是我们有

定理 7 假如 R 不是根基环，那末 R 有极大左理想子环．

在讨论环时，下面这样的理想子环是常常需要的．

定义 3 假如 L 是环 R 的左理想子环，如果 R 中有元 e，对于 R 中任意元 r，有 $r-re\in L$，即 $r\equiv re(L)$，那末 L 叫做 R 的**正则左理想子环**，e 叫做 R 对于 L 的右单位元．

譬如在偶数环 R 中，理想子环(6)是正则理想子环，$e=4$ 是 R 对于(6)的单位元，理想子环(4)不是正则理想子环．

显然，当 R 有单位元时，它的任意左理想子环是正则左理想子环．假如环 R 的左理想子环包含 R 的某正则左理想子环，那末它自身也是正则左理想子环．也就是说，正则左理想子环的扩张左理想子环仍然是正则左理想子环．

下面主要是介绍根基的性质．

定理 8 假如 J 是环 R 的根基，那末 J 是 R 的所有极大正则左理想子环 M_i 的交集，即

$$J=\cap M_i.$$

证明 假定 $a\in\cap M_i$，即 a 在 R 的任意极大正则左理想子环中．如果 a 不是左拟正则元，那末$\{ra+r\}$不包含 a．命 M 是包含$\{ra+r\}$而不包含 a 的极大左理想子环．因为 $r-r(-a)=r+ra\in M$，所以 M 是正则．于是 M 是极大正则左理想子环．因此 $a\in M$，这与假设不合，所以 a 是左拟正则元．于是 $\cap M_i$ 是 R 的拟正则左理想子环．因此 $\cap M_i\subseteq J$．

假如 $a\in J$，那末对于 R 中任意元 r，ra 是左拟正则元．如果 $a\bar{\in}\cap M_i$，那末 R 中有某极大正则左理想子环 M 不包含 a，因为 M 是极大左理想子环，所以由 M 及 a 生成的左理想子环就是 R

自身，即 $R=\{m+(ra+na)\}$，这里 $m\in M$，$r\in R$，n 是整数或零。再假定 e 是 R 关于 M 的右单位元，那末我们有

$$-e=m+(ra+na),$$

于是 $-e^2=em+e(ra+na)$，但 $e(ra+na)$ 是 R 的左拟正则元，所以在 R 中有元 u 存在，使

$$e(ra+na)+u+ue(ra+na)=0.$$

因为

$$-ue^2=uem+ue(ra+na),$$

所以

$$uem-e(ra+na)-u+ue^2=0.$$

再因为对于 R 中任意元 r，$r-re\in M$，所以 $ue-ue^2$ 及 $u-ue$ 都在 M 中，因此 ue^2-u 也在 M 中．又因为 M 是左理想子环，所以 $uem\in M$，因此 $e(ra+na)\in M$．于是 $-e^2=em+e(ra+na)\in M$．但 $e-e^2\in M$，所以 $e\in M$．因此 re 及 $re-r$ 都在 M 中．于是 $-r\in M$，即 $r\in M$．所以 $M=R$，这与假设矛盾，因此 $J\subseteq\cap M_i$，所以 $J=\cap M_i$．于是定理成立．

假如 R 有单位元，那末它的左理想子环都是正则左理想子环，因此 R 的根基 J 是 R 的所有极大左理想子环的交集．

假定 M 是 R 的左理想子环，显然

$$(M:R)=\{r\mid r\in R,\ rR\subseteq M\}$$

是 R 的理想子环．如果 N 是 R 的理想子环，并且 $N\subseteq M$，那末 $NR\subseteq M$，因此 $N\subseteq(M:R)$，这就是说，R 的理想子环如果包含在 M 中，它也包含在 $(M:R)$ 中．假如 $(M:R)\subseteq M$，那末 $(M:R)$ 就是 R 中包含在 M 的最大理想子环．

定理 9 假定 M 是环 R 的正则左理想子环（不一定是极大的），那末 $(M:R)\subseteq M$，因此 $(M:R)$ 是 R 中包含在 M 的最大理想子环．

证明 假定 $a\in(M:R)$，那末 $aR\subseteq M$，如果 e 是 R 对于 M

的右单位元，那末 $a-ae\in M$，因为 $ae\in M$，所以 $a\in M$．于是 $(M:R)\subseteq M$．因此定理成立．

我们知道，满足极小条件的环的构造归结为单纯环的构造，与这类似，一般环的构造归结于本原环的构造．下面介绍的本原环是一类非常重要的环．

定义 4 假如 M 是 R 的极大左理想子环，如果 $(M:R)=0$，那末 R 叫做(左)**本原环**．假如 N 是 R 的理想子环，如果 $R-N$ 是本原环，那末 N 叫做 R 的(左)**本原理想子环**．

显然，本原环的零理想子环是本原理想子环．再体 K 是本原环，因为它的极大左理想子环是零理想子环，并且 $((0):K)=0$．

一个左本原环是否又是右本原环，这是环论中长期没有得到解决的一个问题，1964 年柏尔门(G. M. Bergman)给出了一个左本原环但不是右本原环的例[10]解答了这问题．

定理 10 假定 M 是 R 的极大正则左理想子环，那末 $(M:R)$ 是本原理想子环．

证明 由定理 9，我们得知 $(M:R)\subseteq M$，如果 $(M:R)=M$，那末 M 是 R 的理想子环，因此 $R-M$ 没有非零的左理想子环．这是因为，假如 $L-M$ 是 $R-M$ 的非零左理想子环，那末 L 是 R 的左理想子环，并且 $L\supset M$．因为 M 是正则，所以 L 也是正则，于是 L 是包含 M 的正则左理想子环，这与 M 是极大的假设不合，因此 (0) 是 $R-M$ 的极大左理想子环．再 $((0):(R-M))=0$，这是因为，如果 $\bar{a}\bar{R}=\bar{0}$，那末 $aR\subseteq M$，因此 $a\in(M:R)=M$．所以 $\bar{a}=\bar{0}$，于是 $R-M$ 是本原环，所以 $M=(M:R)$ 是本原理想子环．

如果 $(M:R)\subset M$，显然 $M-(M:R)$ 是 $R-(M:R)$ 的左理想子环，因为 M 是 R 的极大左理想子环，所以 $M-(M:R)$ 又是 $R-(M:R)$ 的极大左理想子环．再 $((M-(M:R)):(R-(M:R)))=0$．这是因为，假如 $\bar{a}\bar{R}\subseteq\overline{M}$，那末 $aR\subseteq M$，因此 $a\in(M:R)$，所以

$\bar{a}=\bar{0}$，于是 $R-(M:R)$ 是本原环．因此 $M:R$ 是本原理想子环．

于是定理成立．

定理 11　环 R 的根基 J 是 R 的所有本原理想子环的交集．

证明　因为 J 是 R 的所有极大正则左理想子环的交集．又因为 R 的任意极大正则左理想子环 M 包含本原理想子环 $(M:R)$，所以 J 包含 R 的某些本原理想子环的交集，因此 J 更包含 R 的所有本原理想子环的交集．下面我们来证明，J 包含在 R 的任意本原理想子环中，因此 J 就是 R 的所有本原理想子环的交集，于是定理就告成立．

假定 N 是 R 的任意本原理想子环，那末 $R-N$ 是本原环．因此 $R-N$ 有极大左理想子环 $M-N$，使 $(M-N:R-N)=\bar{0}$．于是 $(M:R)\subseteqq N$．

如果 M 是正则，那末 M 就是 R 的极大正则左理想子环，因此 $J\subseteqq M$．所以 $J\subseteqq(M:R)$，于是 $J\subseteqq N$．

如果 M 不是正则，因为 $N\subseteqq M$，所以 $(M:R)\subseteqq M$．因此 $(M:R)$ 就是 R 中包含在 M 的最大理想子环．假如 J 不包含在 N 中，那末它也不包含在 $(M:R)$ 中，因此它也不包含在 M 中．如果我们能够证明 $J\subseteqq M$，那末 $J\subseteqq N$，定理就得证．

我们先证明 $\{r|r\in R,\ Rr\subseteqq M\}=M$．这是因为，左边是 R 的左理想子环，并且包含 M，因为 M 是极大，所以它是 M 或者是 R．如果它是 R，那末 $RR\subseteqq M$，因此 $(M:R)=R$，但 $(M:R)\subseteqq M$，所以 $M=R$，这与假设不合．因此它是 M．

再用反证法．假设 $J\subseteqq M$，并且 $a\in J$，$a\bar{\in}M$．如果 $aR\subseteqq M$，那末 $a\in(M:R)\subseteqq M$，这不可．因此 $aR\not\subseteqq M$．命 $b\in R$，$ab\in M$，因为 $\{r|r\in R,\ Rr\subseteqq M\}=M$，所以 $Rab\in M$．但 M 是极大，因此 $(M,\ Rab)=R$．于是存在 $m\in M$，$r\in R$，使 $m+rab=-b$，即 $b+rab=-m\in M$．再因为 $a\in J$，所以 ra 是左拟正则元，因此有

元 c 使 $ra+c+cra=0$. 于是

$$b=b+(ra+c+cra)b=(b+rab)+c(b+rab)\in M.$$

这与 $ab\notin M$ 的假设矛盾. 因此 $J\subseteq M$.

于是定理成立.

因为本原环的零子环是本原理想子环，所以本原环的根基是零,这就是说,本原环是半单纯环. 除零环外,根基环不是本原环.

定理 12 单纯环是根基环或是本原环.

证明 因为 R 是单纯环,所以 $R^2=0$ 或 $R^2=R$. 如果 $R^2=0$, 那末 R 是幂零环，因此它是根基环. 如果 $R^2=R$, 那末 R 不是根基环，因此有极大左理想子环 M. 于是 $(M:R)$ 是 R 的理想子环. 所以 $(M:R)=0$ 或 $(M:R)=R$. 如果 $(M:R)=R$, 那末 $RR=R^2\subseteq M$, 即 $R^2=R\subseteq M$,这与 $M\subset R$ 的假设矛盾. 因此 $(M:R)=0$. 所以 R 是本原环. 于是定理成立.

有没有单纯根基环存在是环论中一个悬而未决的问题，1961 年沙士亚大 (E. Sasiada) 预言这种环是存在的，1967 年他给出一个具体的例来说明[11]，但他给出的不是幂零元环. 因此现在存在的问题是有没有单纯幂零元环.

单纯环如果有单位元就是本原环，因为有单位元的环不是根基环.

定理 13 假定单纯环 R 有极大左理想子环 M 或极小左理想子环 L, 那末 R 是本原环.

证明 假如 R 有极大左理想子环 M，同上定理的证明一样，得知 R 是本原环. 下面我们来证明 R 有极小左理想子环 L 的情况.

命 $N=\{r\mid r\in R,\ rL=0\}$, 那末 N 是 R 的理想子环，因此 $N=R$ 或 $N=0$. 如果 $N=R$, 那末 $RL=0$. 于是右零化 R 的理想子环异于零,所以 R 也零化自身，即 $R^2=0$,因此 L 也是 R 的理

想子环，这与 $L\neq 0$ 的假设不合．所以 $N=0$．于是 $R^2\neq 0$，因此 $R^2=R$，由上定理的证明，R 是本原环．

于是定理得证．

习 题 7.5

1．假定 a 是 R 中元，如果 $-a^2$ 是左拟正则元，那末 a 也是 R 的左拟正则元．

2．假定 $x\in R$．如果 Rx，xR 或 RxR 有一在 R 的根基 J 中，那末 $x\in J$．

3．假如环 R 的根基是 J，$a\in R$，如果 $RaR\in J$，那末 $a\in J$．

4．假如 a，b 是环 R 中元，如果 ab 是左拟正则元，那末 ba 也是左拟正则元．

5．假如 a 是环 R 的根基 J 中元，那末 R 中满足 $x=ax$ 的元 x 只有零元，即 $x=0$．

6．假如 a 是环 R 的根基 J 中元，如果 $a^n=a^m$，$n>m$，那末 $a^m=0$．

7．环 R 中元 a 是左拟正则元的必要充分条件是：拟正则左理想子环 $L=\{r+ra\mid r\in R\}=R$．

8．任意正则左理想子环能够嵌入极大正则左理想子环．

9．假定 R 是根基环，那末它没有正则左理想子环．

10．假定 R 是所有这样的有理数 $\frac{n}{m}$ 构成的环，其中 m 是奇数，n 是任意整数．试证 R 的根基是(2)，它不包含非零的幂零元．

11．假如 R 是有单位元的环，如果其中不是可逆元的元形成理想子环 N，那末 N 是 R 的根基．

12．试证 $J(eRe)=eJ(R)e$，这里 e 是环 R 的幂等元．

§7.6 次 直 和

我们知道根基是零的环叫做半单纯环．这节我们讨论半单纯环的构造，它是 §7.3 中幂零半单纯环构造的推广．

我们先介绍次直和这个新概念，以备引用．在§5.4中我们讨论了环的直和，但是很多时候，环不能写成为若干个环的直和，却能够写成为若干个环的直和的子环，这样把直和推广就创造了次直和这个概念[12]．

假定有两个环

$$R_1=\{0_1,\ 1_1\},\quad R_2=\{0_2,\ 1_2,\ 2_2,\ 3_2\},$$

那末 $$S_1=\{(0_1,\ 0_2),\ (1_1,\ 1_2),\ (0_1,\ 2_2),\ (1_1,\ 3_2)\},$$

$$S_2=\{(0_1,\ 0_2),\ (0_1,\ 2_2),\ (1_1,\ 0_2),\ (1_1,\ 2_2)\}$$

都是 R_1, R_2 的直和 $R_1\dotplus R_2$ 的子环．但它们有区别，在 S_2 中，R_1 中元都出现而 R_2 中元不完全出现．在 S_1 中，R_1, R_2 中元都完全出现，这时显然

$$(0_1,\ 0_2)\to 0_1,\ (1_1,\ 1_2)\to 1_1,\ (0_1,\ 2_2)\to 0_1,\ (1_1,\ 3_2)\to 1_1$$

是 S_1 射到 R_1 上的同态，

$$(0_1,\ 0_2)\to 0_2,\ (1_1,\ 1_2)\to 1_2,\ (0_1,\ 2_2)\to 2_2,\ (1_1,\ 3_2)\to 3_2$$

是 S_1 射到 R_2 上的同态．也就是说，这时 $S_1\sim R_i$, $i=1,\ 2$，但 S_2 就没有这个性质，我们把 S_1 叫做 R_1, R_2 的次直和．一般我们有

定义 假定 $\{R_i\}$, $i=1,\ 2,\ \cdots$，是环 R_i 的集合，R 是 R_i 的直和 $R_1+R_2+\cdots$ 中由

$$r=(r_1,\ r_2,\ \cdots),\quad r_i\in R_i,$$

形成的子环，如果

$$r\to r_i,\quad i=1,\ 2,\ \cdots,$$

是 R 射到 R_i 上的同态，即 $R\sim R_i$，那末 R 叫做 R_i, $i=1,\ 2,\ \cdots$，的次直和．

显然 R_i, $i=1,\ 2,\ \cdots$，的直和是 R_i 的次直和．要注意的是，R_i 的直和是由 R_i 唯一确定的，但 R_i 的次直和不由 R_i 唯一决定，它有各种不同的次直和．

再我们容易得知，R_i 的直和的子环是 R_i 的某子环 R_i' 的次直

和，R_i 的次直和是 R_i 的任意扩张环 R_i^* 的直和的子环.

我们先给出环是次直和的必要充分条件.

定理 1　环 R 是环 R_i, $i=1, 2, \cdots$, 的次直和的必要充分条件是 R 中有理想子环 N_i, $i=1, 2, \cdots$,它们的交集 $\cap N_i=0$,并且 $R_i\cong R-N_i$.

证明　假定 R 是 R_i 的次直和，由定义我们有 $R\sim R_i$, 所以 $R_i\cong R-N_i$, 这里 N_i 是同态核. 因此 N_i 是 R 的理想子环. 再假如 $r=(r_1, r_2, \cdots)\in N_i$, 那末 r_i 是 R_i 的零元，即 $r_i=0$, 因此 $r=(0, 0, \cdots)$，所以 $\cap N_i=0$. 于是条件的必要性成立.

反过来，假如 N_i 是 R 的理想子环，并且 $\cap N_i=0$. 我们命 $R_i=R-N_i$, σ_i 是 R 射到 R_i 上的同态，N_i 是它的同态核. 于是对于 R 中任意元 r, 我们有 $\sigma_i(r)=r_i\in R_i$. 显然在 R_i 的直和 $R_1+R_2+\cdots$中,由所有

$$(r_1, r_2, \cdots), \quad r_i\in R_i$$

形成的环 R' 是 R_i, $i=1, 2, \cdots$,的次直和. 下面我们来证明 R 与 R' 同构.

我们命 R 中元 r 与 $(\sigma_1(r), \sigma_2(r), \cdots)$对应,即

$$r\to(\sigma_1(r), \sigma_2(r), \cdots).$$

显然它是 R 射到 R' 上的映射. 因为

$$\sigma_i(r+s)=\sigma_i(r)+\sigma_i(s), \quad \sigma_i(rs)=\sigma_i(r)\sigma_i(s),$$

所以

$$\begin{aligned} r+s&\to(\sigma_1(r+s), \sigma_2(r+s), \cdots)\\ &=(\sigma_1(r), \sigma_2(r), \cdots)+(\sigma_1(s), \sigma_2(s), \cdots),\\ r\cdot s&\to(\sigma_1(rs), \sigma_2(rs), \cdots)\\ &=(\sigma_1(r), \sigma_2(r), \cdots)(\sigma_1(s), \sigma_2(s), \cdots). \end{aligned}$$

于是 R 与 R' 同态,即 $R\sim R'$. 再因为 $\sigma_i(r)=0$ 时，$r\in N_i$, $i=1, 2, \cdots$. 但 $\cap N_i=0$,所以 $r=0$. 因此 $R\cong R'$. 这就是说，R 与 R_i, $i=1, 2, \cdots$,的次直和同构,所以条件的充分性成立.

于是定理得证.

下面是贾柯勃逊关于半单纯环的主要构造定理.

定理 2 半单纯环是本原环的次直和.

证明 根据§7.5定理11, R 的所有本原理想子环 N_i 的交集 $\cap N_i=0$, 于是由上定理, R 是 $R-N_i$ 的次直和. 又因为 N_i 是 R 的本原理想子环,所以 $R-N_i$ 是本原环. 因此定理成立.

于是我们又得到

定理 3 假定环 R 的根基是 J, 那末 $R-J$ 是本原环的次直和.

最后我们介绍可换环的几个重要推论.

定理 4 可换本原环是体.

证明 假定 R 是本原环, M 是它的极大左理想子环, $(M:R)=0$. 因为 R 是可换, 所以 $M\subseteq(M:R)\subsetneq R$, 因此 $M=0$. 这就是说,零理想子环是 R 的极大理想子环,即 R 除零理想子环外,没有其他理想子环. 再因为 R 的根基是零,所以它不是幂零元环. 于是由§3.6定理1, R 是体. 因此定理成立.

由定理2及上定理我们又得到

定理 5 元数大于1的可换半单纯环是可换体的次直和.

下面是比这广泛的定理,由后面的定理7, 我们立即推得

定理 6 假如可换环不含非零的幂零元, 那末它是整环的次直和.

证明 假定环 R 没有非零的幂零元,由后面的定理7, 得知 R 的所有质理想子环 P_i, $i=1, 2, \cdots$, 的交集是零. 于是由定理1, 环 R 是 $R-P_i$ 的次直和. 因为 P_i 是质理想子环, 所以 $R-P_i$ 是整环. 因此 R 是整环 $R-P_i$ 的次直和. 于是定理成立.

定理 7 可换环 R 的所有质理想子环的交集是 R 中所有幂零元形成的理想子环.

证明 因为任意幂零元都包含在任意质理想子环中，所以 R 的所有质理想子环的交集包含 R 的所有幂零元. 假如我们能够证明 R 中任意非幂零元 r 不包含在 R 的某质理想子环中，那末定理就告成立.

假如 M 是 R 中所有不含 r 的各幂的理想子环的集合. 显然 M 不是空集，因为 M 中至少包含零理想子环. 由冲恩引理，M 中有极大理想子环 P，这 P 就是质理想子环. 这是因为，假如 a, b 是 R 中元，但都不在 P 中，那末 $(P, a)\supset P$, $(P, b)\supset P$, 因为 P 是极大，所以 $r^m\in(P, a)$, $r^n\in(P, b)$. 于是 $r^{m+n}\in(P, a)(P, b)=(P, ab)$，但 $r^{m+n}\notin P$，所以 $ab\notin P$，因此 P 就是不包含 r 的质理想子环. 于是 R 的所有质理想子环的交集只含 R 的所有幂零元. 因此定理成立.

此外我们还知道，一个环是体 $Z-(2)$ 的次直和的必要充分条件是：它是布尔环. 一个环，如果它的特征数是质数 p，并且对于任意元 a 有 $a^p=a$，那末这环就叫做 **p 环**. p 环是有单位元的可换环. 一个环是体 $Z-(p)$ 的次直和的必要充分条件是：它是 p 环. 这些的证明我们从略[13].

习 题 7.6

1. 在可换环中，本原理想子环是质理想子环，但质理想子环不一定是本原理想子环，这是为什么？

§7.7 本原环，稠密环

我们知道，假如 M 是环 R 的极大左理想子环，如果 $(M:R)=0$，那末 R 就是本原环. 前面我们已经介绍了本原环，这节我们将进一步讨论本原环的构造，主要就是证明下面著名的贾柯勃逊密

度定理.

定理 1 假定R是本原环,M是它的极大左理想子环,$(M:R)=0$, E是$\bar{R}=R-M$的自同态环. R'是E中与R同构的子环, D是E中所有与R'中任意元能够交换的元形成的体. 那末R是D的向量空间$\bar{R}$的稠密环.

下面我们来分段证明.

首先我们来建立R'. 因为M只是R的左理想子环而不是理想子环,所以$\bar{R}=R-M$只是加群,一般不成为环. 假定a'是把$\bar{R}$中元$\bar{r}$变为$\overline{ar}$, $a\in R$, 的自同态,那末E中所有象a'这样的自同态构成与R同构的子环R'. 这是因为由$a'+b'=(a+b)'$, $a'b'=(ab)'$,显然$a\to a'$是R射到R'上的同态. 再因为$a'=0$时$\overline{ar}=\bar{0}$, 即$ar\in M$,所以$a\in(M:R)=0$. 因此上述同态是同构. 于是$R\cong R'$.

再我们来证明D是体.

定理 2 假定D是E中所有与R'中任意元能够交换的元集合,即

$$D=\{\alpha|\alpha\in E,\ \alpha r'=r'\alpha,\ r'\text{是}R'\text{中任意元}\},$$

那末D是体.

证明 D显然是环. 并且有单位元,因为E有单位元.

假定α是D中非零元, 那末$\{\alpha\bar{r}\}$是$\bar{R}=R-M$对于α的象集,我们先来证明$\{\alpha\bar{r}\}=\bar{R}$, 因此$\alpha$是$\bar{R}$射到$\bar{R}$上的自同态.

因为$\alpha\neq0$,所以$\{\alpha\bar{r}\}\neq\bar{0}$. 因此$\bar{R}$中有元使$\alpha\bar{r}\neq\bar{0}$, 即$\alpha r\notin M$. 又因为$M$是极大左理想子环,所以由$M$及$\alpha r$生成的左理想子环就是$R$. 于是对于$R$中任意元$x$,我们就有

$$x=m+a\alpha r+n\alpha r,\quad m\in M,\ a\in R,\ n\text{是整数}.$$

因为$\alpha\in D$, 所以$a\alpha r=\alpha ar$, 因此$x=m+\alpha(ar+nr)$, 于是$\bar{x}=\alpha(\overline{ar}+n\bar{r})$,这就是说, 对于$\bar{R}$中任意元$\bar{x}$, 我们有$\bar{x}\in\{\alpha\bar{r}\}$, 所以

$\{\alpha\bar{r}\}=\bar{R}$.

再我们来证明 α 是 $\bar{R}$ 的自同构.

假定 $\alpha\bar{r}=\bar{0}$,那末 $ar\in M$,如果 $r\bar{\in} M$,因为 M 是极大左理想子环,所以 R 中任意元 x 可以写成

$$x=m+ar+nr,\quad m\in M,\quad a\in R,\quad n \text{ 是整数}.$$

因此

$$\alpha x=\alpha m+\alpha ar+\alpha nr=\alpha m+a\cdot\alpha r+n\alpha r\in M,$$

即 $\alpha\bar{x}=\bar{0}$,这与 $\alpha\neq 0$ 的假设不合. 于是 $r\in M$. 这就是说,$\alpha\bar{r}=\bar{0}$ 时 $\bar{r}=\bar{0}$,所以 α 是同构.

于是在 E 中 α 有逆 α^{-1},因为 $\alpha r'=r'\alpha$,所以 $\alpha^{-1}r'=r'\alpha^{-1}$,因此 $\alpha^{-1}\in D$. 于是 D 是体,所以定理成立.

因为 D 中元是 $\bar{R}$ 的自同态,所以 $\bar{R}$ 是 D 的向量空间,于是我们有

定理 3 $\bar{R}=R-M$ 是体 D 的左向量空间,R' 中元是 D 空间 $\bar{R}$ 的线性变换.

$\bar{R}$ 一般虽是 D 的无穷维空间,但 R' 中元是 D 空间 $\bar{R}$ 的线性变换. 我们可以同 §7.4 中一样,把 R' 中元用元素是 D 中元的无穷阶矩阵表示. 我们不这样做,因为这样我们就无法再推得其他性质,我们用另一个概念来表达.

下面我们介绍一个重要概念.

定义 假定 V 是体 D 的(左)向量空间,T 是 V 的线性变换集合,如果对于 V 中 n 个任意线性无关的元 $x_1,\cdots,x_n$ 及任意 n 个元 $y_1,\cdots,y_n$,在 T 中有把 $x_i\to y_i$ 的线性变换,那末 T 叫做对于 V 是 **n 重可迁**. 如果对于任意 n,T 对于 V 都是 n 重可迁,那末 T 叫做对于 V 是**稠密的**. 假如 T 又成环,那末 T 又叫做 V 的稠密环,或简称稠密环.

这里 V 一般是无穷维空间而不是有穷维空间. 假如 V 是 D

的 n 维空间，由线代数得知，V 的所有线性变换形成的环就是全矩阵环 D_n. 又因为在 V 的线性变换中有把 V 中任意 n 个线性无关的元变为任意 n 个元的线性变换，因此 D_n 是 V 的稠密环，于是满足极小条件的非幂零单纯环是稠密环. 因此魏特邦-阿丁第二构造定理是密度定理的特例.

下面我们来证明 R' 是 D 空间 $\bar{R}$ 的稠密环.

假定 $x\neq 0$, $\bar{x}\in\bar{R}$, 那末 $R'\bar{x}=\bar{R}$, 这是因为 R' 中元 a' 是把 $\bar{x}$ 变为 $\overline{ax}$ 的自同态. 所以 $R'x$ 是 R' 空间 $\bar{R}$ 的子空间. 又因为 M 是 R 的极大左理想子环，所以 $\bar{R}$ 是 R' 的既约空间. 因此 $R'x=0$ 或 $R'x=\bar{R}$. 如果 $R'\bar{x}=0$, 那末由 x 生成的空间是 $\bar{R}$ 的真子空间，这与 $\bar{R}$ 是 R' 的既约空间矛盾. 所以 $R'x=\bar{R}$, 于是对于 $\bar{R}$ 中任意元 $x\neq 0$, y, 在 R' 中有元 r' 使 $r'x=\bar{y}$. 这就是说，R' 对于 D 空间 $\bar{R}$ 是 1 重可迁.

再假定 $\bar{x}_1, \cdots, \bar{x}_n$ 是 $\bar{R}$ 中 n 个线性无关的元，$\bar{y}_1, \cdots, \bar{y}_n$ 是 $\bar{R}$ 中任意 n 个元，如果在 R' 中能够找到 a'_i 使

$$a'_i\bar{x}_i\neq 0,\quad a'_i\bar{x}_j=0,\quad i\neq j,$$

因为 R' 已是 1 重可迁，所以在 R' 中有元 b'_i, $i=1,\cdots,n$, 存在，使

$$b'_i(a'_i\bar{x}_i)=\bar{y}_i.$$

命 $a'=b'_1a'_1+\cdots+b'_na'_n$, 那末

$$a'\bar{x}_i=(b'_1a'_1+\cdots+b'_na'_n)\bar{x}_i=b'_ia'_i\bar{x}_i=\bar{y}_i,$$

因此只要下面的定理成立，R' 就是 $\bar{R}$ 的稠密环了.

定理 4 假定 W 是 D 空间 $\bar{R}=R-M$ 的 n 维子空间，$x\in\bar{R}$, $x\bar{\in}W$, 那末 R' 中有元 a 使 $aW=0$, $ax\neq 0$.

证明 我们用归纳法来证明.

当 $n=0$ 时 $W=0$, 这时 $R'W=0$. 根据前面证得性质，对于 $x\neq 0$ 有 $R'x=\bar{R}$, 这就是说，R' 中有元 a 使 $aW=0$, $ax\neq 0$, 因此 $n=0$ 时定理成立.

假定对维数 $<n$ 的子空间定理成立，下面我们来证明 W 的维数是 n 时定理仍成立.

我们把 W 写成

$$W=W_1+Dy,$$

这里 W_1 是 D 空间 $\bar{R}$ 的 $n-1$ 维子空间. 命 R' 中所有零化 W_1 的集合为 S, 即 $SW_1=0$. 根据归纳法假设, $Sy\neq0$, 显然 S 是 R' 的左理想子环, 因此 Sy 是 R' 空间 $\bar{R}=R-M$ 的子空间. 所以 $Sy=\bar{R}$. 假如 R' 中零化 W 的元也同时都零化 x, 我们命 $ay\rightarrow ax, a\in S$, 那末这映射是 R' 空间 $\bar{R}$ 的自同态. 这是因为, 由 $a_1y\rightarrow a_1x$, $a_2y\rightarrow a_2x$, 如果 $a_1y=a_2y$, 那末 $(a_1-a_2)y=0$, 但 $a_1-a_2\in S$, 所以 a_1-a_2 零化 W_1, 同时又零化 y, 因此零化 W. 根据假设, 它也零化 x, 即 $a_1x=a_2x$. 用 α 表示这自同态, 于是 $\alpha(ay)=ax$. 再由 $\alpha(r'ay)=r'ax$, 得 $\alpha(r'(ay))=r'(\alpha(ay))$, 所以 $\alpha r'=r'\alpha$, 即 α 与 R' 中任意元能够交换, 因此 $\alpha\in D$. 于是 $a(x-\alpha y)=0$, 即 $S(x-\alpha y)=0$. 根据归纳法假设, $x-\alpha y\in W_1$, 所以 $x\in W_1+\alpha y\in W$. 这与 $x\bar{\in}W$ 的假设矛盾. 因此 R' 中零化 W 的元不同时都零化 x, 所以定理成立.

于是上面的密度定理完全得证.

假定 V 是体 D 的向量空间, R 是 V 的线性变换形成的环, 根据上面密度定理的证明, 如果下面两个条件成立: (i) R 对于 V 是 1 重可迁; (ii) V 的自同态环 E 中所有与 R 中任意元能够交换的元形成的环就是 D, 那末 R 就是 V 的稠密环.

定理 5　假定 V 是体 K 的向量空间, R 是 V 的线性变换形成的环, 如果 R 对于 V 是 2 重可迁, 那末 R 是稠密环.

证明　只要我们证明在 V 的自同态环中所有与 R 中任意元能够交换的元 s 是在 K 中, 那末 R 就是 V 的稠密环了.

假定 x 是 V 中非零的元, 如果 x, sx 线性无关, 那末在 R 中

有元 r，使 $rx=0$．$rsx\neq 0$，于是 $srx\neq 0$，这与 $rx=0$ 矛盾．所以 x，sx 线性相关．于是在 K 中有元 α_x 使

$$\alpha_x x = sx.$$

再假设 $y\neq 0$，同样我们有 $\alpha_y y = sy$．命 $y=ax$，$a\in R$．于是

$$\alpha_y y = sy = s(ax) = a(sx) = a(\alpha_x x) = \alpha_x(ax) = \alpha_x y.$$

所以 $\alpha_x=\alpha_y$．即 $s=\alpha_x$，这就是说 s 是 K 中元．于是定理成立．

下面是密度定理的逆．

定理 6　假定 V 是体 K 空间，R 是 V 的线性变换形成的环，如果 R 是 V 的 1 重可迁，那末 R 是本原环．

证明　假定 $v\neq 0$ 是 V 中任意元，因为 R 是 V 的 1 重可迁，所以 $Rv=V$．命 $M=\{r\in R\,|\,rv=0\}$，显然 M 是 R 的左理想子环，并且 $M\neq R$．于是 $(M:R)=\{r\in R\,|\,rR\subseteq M\}=0$，这是因为，由 $rR\subseteq M$ 得 $rRv=0$，即 $rv=0$，这就是说，r 把 V 中任意元变为 0，因此 $r=0$．

下面我们再证明 M 是 R 的极大左理想子环．假定 R 的左理想子环 $N\supset M$，那末 R 中有元 $x\in N$，$x\overline{\in} M$，因此 $xv\neq 0$．于是 $Rxv=V$，因为 $Rx\subseteq N$，所以 $Nv=V$．假定 r 是 R 中任意元，$rv=v_1$，那末 N 中有元 n 使 $nv=v_1$，于是 $nv=rv$，即 $(n-r)v=0$，因此 $n-r\in M$．所以 $r=n-m\in N$，这就是说 $R\subseteq N$，于是 $R=N$，因此 M 是 R 的极大左理想子环．

于是 R 是本原环，所以定理成立．

要注意的是，这时 R 不一定是 K 空间 V 的稠密环，一般它是包含 K 的体 D 的空间 V 的稠密环．譬如 V 是复数体看成实数体 F 的向量空间，R 是复数体看成为 F 的空间 V 的线性变换形成的环，对于 $0\neq v\in V$，显然 $Rv=V$．因此 R 是 V 的 1 重可迁，所以 R 是本原环．但 R 不是 F 的空间 V 的稠密环．这是因为，1，i 是 V 中对于 F 线性无关的元，并且 R 中不存在使 $(a+bi)1=1$，

$(a+bi)i=1$ 的元 $a+bi$，所以 R 对于 F 的 V 不是 2 重可迁，因此 R 不是 F 的 V 的稠密环．再我们容易得知(后面习题 2)，在 V 的自同态环中，所有与 R 中任意元能够交换的元形成的体是复数体，即 $D=R$，于是 R 是对于 R 的 V 的稠密环．

由上定理我们立即推得，假如 R 是向量空间 V 的线性变换形成的稠密环，那末 R 是本原环．

根据上面密度定理我们不难得到下面本原环的两个性质．

定理 7　假定 R 是本原环，如果 R 中任意元的平方是 R 的左拟正则元，那末 R 是体．

证明　假定 R 是体 D 向量空间 V 的稠密环，如果能够证明 V 的维数是 1，那末 R 就是体了．

假定 x, y 是 V 中任意两个线性无关的元，那末 R 中有元 a 使

$$ax=y,\quad ay=-x,$$

即

$$a^2x=-x,\quad a^2y=-y.$$

但 a^2 是 R 的左拟正则元，因此在 R 中有元 b 使 $a^2+b+ba^2=0$，于是

$$(a^2+b+ba^2)x=a^2x+bx+ba^2x=-x,$$

即 $x=0$，这与 x, y 线性无关的假设矛盾．这就是说 V 中任意两个元都线性相关，所以 V 的维数是 1．于是定理成立．

定理 8　假定 R 是本原环，并且对于 R 中任意两元 a, b 有 $a(ab-ba)=(ab-ba)a$，那末 R 是体．

证明　假定 x, y 是 V 中任意两个线性无关的元，那末 R 中有元 a, b 使

$$ax=y,\quad ay=-x,\quad bx=y,\quad by=x,$$

由计算得

$$a(ab-ba)x=-2y,\quad (ab-ba)ax=2y,$$

于是 $-2y=2y$，即 $2y=0$，所以 $y=0$，这与 x, y 线性无关的假设不

合. 因此 V 的维数是 1. 所以 R 是体, 于是定理成立.

最后介绍满足极小条件的环的两个重要性质.

定理 9 满足极小条件的本原环是单纯环.

证明 假如本原环 R 满足极小条件, 如果我们能够证明 $\bar{R}=R-M$ 是 D 的有穷维空间, 那末定理就告成立. 下面我们用反证法来证明.

假定 $\bar{R}$ 中有无穷个线性无关的元 x_i, $i=1, 2, \cdots$, 因为 R 中所有零化 $x_1, \cdots, x_n$ 的元形成 R 的左理想子环 L_n, 由定理 4, $L_i\neq L_j$, $i\neq j$. 于是 R 的左理想子环列

$$L_1\supset L_2\supset\cdots\supset L_n\supset\cdots$$

有无穷项, 这与 R 满足极小条件的假设不合. 因此 D 空间 $\bar{R}$ 是有穷维的. 于是定理成立.

由 §7.6 定理 2, 我们得知半单纯环是本原环的次直和, 假如环又满足极小条件, 我们就有

定理 10 满足极小条件的半单纯环是有穷个单纯环的直和.

证明 假定 R 是半单纯环, 它与本原环 $R-N_i$, $i=1, 2, \cdots$ 的次直和同构. 这里 N_i 是 R 的理想子环. 因为 R 又满足极小条件, 所以

$$N_1\supset N_1\cap N_2\supset\cdots$$

只有有穷项. 但 $\cap N_i=0$, 因此我们有有穷个 N_i, 譬如 $N_1, \cdots, N_n$, 使 $\bigcap\limits_{i=1}^{n} N_i=0$, 但 $M_i=\bigcap\limits_{j\neq i} N_j\neq 0$. 再由定理 9, 本原环 $R-N_i$ 是单纯环, 所以 N_i 是 R 的极大理想子环. 于是 $(N_i, M_i)=R$. 因为 $M_i\cap N_i=\cap N_i=0$, 所以 $R=M_i+N_i$. 又因为 $M_i\cong R-N_i$ 而 $R-N_i$ 是单纯环, 所以 M_i 是单纯环. 我们命 $S_k=\bigcap\limits_{i=1}^{k} N_i$, $k=1, \cdots, n$, 于是 $R=M_1+N_1=M_1+S_1$. 如果我们能够证明, 对于任意 $k<n$,

$S_k=M_{k+1}+S_{k+1}$，因为 $S_n=0$，我们就得到 $R=M_1+\cdots+M_n$，即 R 是有穷个单纯环 M_i 的直和．于是定理成立．

因为 $S_k\subsetneqq N_{k+1}$ 而 N_{k+1} 是 R 的极大理想子环，所以 $R=(S_k, N_{k+1})$．于是由第二同构定理(§5.2)，

$$R-N_{k+1}=(S_k,\ N_{k+1})-N_{k+1}$$

$$\cong S_k-(S_k\cap N_{k+1})=S_k-S_{k+1},$$

所以 S_k-S_{k+1} 是单纯环．因此 S_{k+1} 是 S_k 的极大理想子环．再因为 $M_{k+1}\nsubseteq S_{k+1}$，$M_{k+1}\subseteq S_k$，所以 $S_k=(S_{k+1},\ M_{k+1})$，又因为 $S_{k+1}\cap M_{k+1}=0$，所以 $S_k=M_{k+1}+S_{k+1}$．

因此定理成立．

于是§7.3魏特邦-阿丁第一构造定理是§7.6定理2的特例．贾柯勃逊根基是幂零根基最好的推广，所得到的关于单纯环构造的密度定理也是魏特邦-阿丁第二构造定理最好的推广．半单纯环的构造定理也是魏特邦-阿丁第一构造定理最好的推广，其中引为不足的是本原环远不及单纯环简单．1947年勃朗(B. Brown)及麦珂把贾柯勃逊根基概念推广，建立了另一个根基概念，叫做**勃朗-麦珂根基**[14]．假如环 R 的勃朗-麦珂根基是 G，那末 $R-G$ 是有单位元的单纯环的次直和．这结果与魏特邦-阿丁第一构造定理更为接近，但勃朗-麦珂根基较贾柯勃逊根基复杂，不及贾柯勃逊根基自然，这是勃朗-麦珂根基不足之处．

习　题　7.7

1．假定 V 是体 K 向量空间，R 是 V 的所有线性变换形成的环，那末 R 是 V 的稠密环．

2．假定 G 是由 (a, b) 形成的加群，这里 $a, b\in F$，F 是实数体，$\alpha=(1, 0)$，$\beta=(0, 1)$，T 是 G 的自同态，

$$T\alpha=a_{11}\alpha+a_{12}\beta,\quad T\beta=a_{21}\alpha+a_{22}\beta,$$

试证 G 的自同态环与全矩阵环 F_2 同构，$T\to\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$是它的同构映射。

3. 本原环是质环。

4. 本原环的中心是整环。

5. 假定 R 是本原环，$L=Re$ 是极小左理想子环，R 是体 D 的向量空间 V 的稠密环，试证 eV 关于 D 的维数是 1。

参考文献

[1] J. H. M. Wedderburn, On hypercomplex members, Proc. London Math. Soc., 6 (1908), 77～117.

[2] E. Artin, Zur Theorie der hyperkomplexen Zahlen, Abh. Math Sem. Univ. Hamburg, 5 (1927), 251～260.

[3] N. Jacobson, The radical and semi-simplicity for arbitrary rings, Amer. J. Math., 67 (1945), 300～320.

[4] (1) 谢邦杰，仑根理想，吉林大学学报，总 4 期(1957)，177～214。
(2) N. J. Divinsky, rings and radicals (1964), 116～156.

[5] N. Jacobson, Structure of rings (1956).

[6] I. Kaplansky, Fields and rings (1972).

[7] C. Hopkins, Rings with minimal conditions for left ideals, Ann. of Math., V. 40 (1939), 712～730.

[8] R. Brauer, On the nilpotency of the radical of a ring, Bull. Amer. Math. Soc., V. 48 (1942), 752～758.

[9] S. Perlis, A characterization of the radical of an algebra, Bull. Amer. Math. Soc., V. 48 (1942), 128～132.

[10] G. M. Bergman, A ring primitive on the right but not on the left, Proc. Amer. Math. Soc., 15 (1964), 473～475. Correction on page 1000.

[11] E. Sadada, P. M. Cohen, An example of a simple radical rings, J. Algebra, 5 (1967), 373～377.

[12] (1) G. Birkhoff, Subdirect unions in universal algebra, Bull. Amer. Math. Soc., 50 (1944), 764～768.
(2) N. H. McCoy, Subdirect sums of rings, Bull. Amer. Math. Soc., 53 (1947), 856～877.

[13] N. H. McCoy, Rings and Ideals (1948), 140～144.

[14] B. Brown, N. H. McCoy, Radicals and subdirect sum, Amer. J. Math., 69 (1947), 46～58.
——, The radical of a ring, Duke Math. J. 15 (1948), 495～499.

习 题 答 案

习题除较简单的外都给解答，但答非常简略，只作为解题思路供读者参考校核。

习 题 1.1

1．任意两个集都有交集与并集．

2．$A\cup B=B$, $A\cap B=A$．

4．i 元集有C_n^i个，空集1个，共有子集$C_n^0+C_n^1+\cdots+C_n^n=(1+1)^n=2^n$．

习 题 1.2

2．这时整数集分为5类：$\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$．

3．如果 τ 有逆 τ^{-1}，那末 $\sigma=\tau^{-1}$．再假如 $\tau(x_1)=y_1$, $\tau(x_2)=y_2$，如果 $y_1=y_2$，那末 $\sigma\tau(x_1)=\sigma\tau(x_2)$，即 $x_1=x_2$．于是 τ 是可逆的，所以有逆．

5．假如不存在使 $a\sim b$ 的 b，那末 $a\sim a$ 就不能成立．

习 题 2.1

1．没有单位元，所以不成群．又因为$(2\cdot3)4\neq2(3\cdot4)$，所以结合律也不成立．

2．成为群，群表为

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

这里 $a=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $b=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$,

$c=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, $d=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$.

3．群表为

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	d	c	f	e
c	c	e	a	f	b	d
d	d	f	b	c	a	
e	e	c	f	a	d	b
f	f	d	e	b	c	a

$a=r$, $\quad b=\dfrac{1}{r}$,

$c=1-r$, $\quad d=\dfrac{1}{1-r}$,

$e=\dfrac{r-1}{r}$, $\quad f=\dfrac{r}{r-1}$.

4. $s^2=(ae)(bc)$, $t^2=(acb)$, $st=(acdb)$

$ts=(acbde)$, $tst^{-1}=(abcd)$, $sts^{-1}=(abe)(cd)$.

5.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	6	5	4	3
3	3	5	1	6	2	4
4	4	6	5	1	3	2
5	5	3	4	2	6	1
6	6	4	2	3	1	5

这里$1=(1)$，$2=(1\,2)$，$3=(1\,3)$，$4=(2\,3)$，$5=(1\,2\,3)$，$6=(1\,3\,2)$。即 $S_3=\{1,\ 5,\ 5^2(=6),\ 4,\ 5\cdot4(=2),\ 5^2\cdot4(=3)\}$

6．因为$(ab)^2=abab=a^2b^2$，所以$ba=ab$。

7　由$(ab)(ab)=e$，$(ab)(ba)=ab^2a=a^2=e$，得$(ab)(ab)=(ab)(ba)$，所以$ab=ba$。

8．因为G是非可换群，所以其中存在$a^{-1}\neq a$的元a，命$b=a^{-1}$，那末$ab=ba$。

9．由$ax=b$在G中有解及消去律得知σ_a是可逆映射．再因为$\sigma_a\sigma_b(g)=\sigma_a(bg)=abg=\sigma_{ab}(g)$，所以$\sigma_a\sigma_b=\sigma_{ab}$。

10．由$3°$，$e/(b/c)=c/b$，因此我们有$(ac^{-1})(cb^{-1})=ab^{-1}$，命$a=x$，$b=e$，$c=y^{-1}$，即得$x=xe^{-1}=(xy)(y^{-1}e^{-1})=(xy)y^{-1}$。又命$a=xy$，$b^{-1}=z$，$c=y$得结合律$(xy)z=((xy)y^{-1})(yz)=x(yz)$。

习　题　2.2

2. $Z-(100)=(\bar{1})$，$(\bar{2})$，$(\bar{4})$，$(\bar{5})$，$(\overline{10})$，$(\overline{20})$，$(\overline{50})$，$(\overline{100})=(\bar{0})$。

5．因为$a^m=1$，$b^n=1$，所以$(ab)^{mn}=1$，因此$r|mn$．再因为$(ab)^{mr}=b^{mr}=1$，$(ab)^{nr}=a^{nr}=1$，所以$n|mr$，$m|nr$．如果$(m,n)=1$，那末$n|r$，$m|r$，因此$mn|r$，所以$r=mn$。

又假如$m=p_1^{s_1}p_2^{s_2}p_3^{s_3}$，$n=p_1^{t_1}p_2^{t_2}p_3^{t_3}$，$t_1\geqslant s_1$，$t_2\leqslant s_2$，$t_3\geqslant s_3$，于是$q=p_1^{t_1}p_2^{s_2}p_3^{t_3}$。但$a^{p_2^{s_2}}$的阶为$p_1^{s_1}p_3^{s_3}$，$b^{p_1^{t_1}p_3^{t_3}}$的阶为$p_2^{t_2}$，所以$a^{p_2^{s_2}}$，$b^{p_1^{t_1}p_3^{t_3}}$的阶为$q$。

6．假如$a^m=1$，$b^n=1$，如果$n\nmid m$，那末m，n的最小公倍$q>m$，于是G中有阶为q的元，这与假设不合。

8．因为任意排列可以写成循环排列的乘积，并且

$(1\,2\cdots n)=(1\,n)(1\,n-1)\cdots(1\,2)$，　$(i\,j)=(1\,i)(1\,j)(1\,i)$。

9. 因为$(1\,j)(1\,i)=(1\,i\,j)$，$(1\,i\,j)=(1\,2\,j)^2(1\,2\,i)(1\,2\,j)$。

10.

$$\begin{array}{ccc} a & \xrightarrow{\tau} & \tau(a) \\ \sigma\downarrow & & \downarrow\sigma \\ \sigma(a) & \xrightarrow[\sigma\tau\sigma^{-1}]{} & \sigma\tau(a) \end{array}$$

即 $\sigma\tau\sigma^{-1}(\sigma(a))=\sigma\tau(a)$。

习 题 2.3

1. $G\ni a\neq e$ 时，(a) 的元数是 G 的元数的因数，因此 $G=(a)$.

2. 对于任一不在 H 中的 a，$G=H\cup aH$，$G=H\cup Ha$，所以 $aH=Ha$.

3. $G=a_1H\cup a_2H\cup\cdots$，$H=b_1K\cup b_2K\cup\cdots$ 时，如果 $a_ib_jK\cap a_kb_lK\neq 0$，那末 $a_ib_j=a_kb_lk$，于是 $a_i=a_kb_lkb_j^{-1}\in a_kH$，所以 $a_i=a_k$ 因此 $b_j=b_l$，即 $i=k$，$j=l$.

4. 假定 $G=(a)$，$H=(a^r)$，于是 $G=H\cup aH\cup\cdots\cup a^{r-1}H$. 所以 $(G:H)=r$.

5. 当 $aH\cdot bH=abH$ 时，$ahb=abh_1$，因此 $bhb^{-1}\in H$.

6. 引用 §2.2 习题 10，得知 (1 2)，(3 4) 互为共轭，(1 3)(2 4)，(1 4)(2 3) 互为共轭，(1 2)(3 4) 自己共轭. 因此 B_8 的中心为 $\{(1),(1\,2)(3\,4)\}$，正规子群有

$$\{(1),(1\,2),(3\,4),(1\,2)(3\,4)\},$$

$$\{(1),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\},$$

$$((1\,4\,2\,3))=((1\,3\,2\,4))=\{(1),(1\,2)(3\,4),(1\,4\,2\,3),(1\,3\,2\,4)\}.$$

8. A_4 的子群，2 元的有 3 个：

$$\{(1),(1\,2)(3\,4)\}=((1\,2)(3\,4)),\ \{(1),(1\,3)(2\,4)\}=((1\,3)(2\,4)),$$

$$\{(1),(1\,4)(2\,3)\}=((1\,4)(2\,3));$$

3 元的有 4 个：

$$((1\,2\,3))=((1\,3\,2)),\ ((1\,2\,4))=((1\,4\,2)),\ ((1\,3\,4))=((1\,4\,3)),$$

$$((2\,3\,4))=((2\,4\,3));$$

4 元的只有 1 个

$$B_4=\{(1),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}.$$

它没有 6 元子群，只有 B_4 是正规子群.

10. 假如 $\tau(i)=j$，$i\neq j$ 时，有适当的 σ 使 $\sigma\tau\sigma^{-1}(i)\neq j$，那末 S_n 的中心就是单位元群. 取 $\sigma=(j,k)$，$k\neq j$，显然 $\sigma\tau\sigma^{-1}(i)=k$.

11. 假设 H 是 S_4 的正规子群，$H\neq S_4$，$H\neq A_4$，$H\neq$ 单位元群，那末

(i) H 不包含奇排列(1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2). 这是因为如果 H 包含(1 2), 那末它也包含(2 3)(1 2)(2 3) = (1 3), (2 4)(1 2)(2 4) = (1 4), 于是 $H = S_4$. 又如果 H 包含(1 2 3 4), 那末它也包含(1 2)(1 2 3 4)(1 2) = (1 3 4 2). 同样它又包含其余四个(1 2 4 3), (1 3 2 4), (1 4 2 3), (1 4 3 2). 于是它包含(1 2 3 4)(1 2 4 3)^2 = (2 4), 再加上单位元群, H 最少包含 13 个元, 因此 $H = S_4$.

(ii) H 不包含偶排列(1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3). 这是因为如果 H 包含(1 2 3), 它也包含(3 4)(1 2 3)(3 4) = (1 2 4), 因此 $H \supseteq A_4$.

(iii) $H = \{(1), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\}$, 这是因为由 § 2.2 习题 10, 二个对换的积的共轭仍为二个对换的积, 但 S_4 中二个对换的积只有上面三个. 因此 H 是 S_4 的正规子群.

12. 假如 H 是 $S_n (n>4)$ 的正规子群, 因为 $H \cap A_n$ 是 A_n 的正规子群, 所以 $H \cap A_n = A_n$ 或 $H \cap A_n$ = 单位元群. 从前者言, $H \supseteq A_n$. 从后者言, H 所包含的元除单位元外都是奇排列, 并且它们的平方又都是单位元. 再这些奇排列用不同文字的循环排列的乘积表示时又都是对换的乘积, 因为不如此, 它们平方就不是单位元. 又 H 不含二个奇排列, 因为二个这样奇排列的乘积是单位元, 于是它们互逆, 因此它们就相等. 假如 $S = (ij) \cdots$ 是 H 所含的奇排列, 命 $t = (ik)$, $k \neq j$, 那末 $tst^{-1} = (kj) \cdots \in H$. 这不可. 所以 H 是单位元群.

习 题 2.4

1. 因为 G 是可换群, 所以除恒等同构外没有内同构. 此外映射有五: (ab), (bc), (ca), (abc), (acb), 由群表得知 a, b, c 中任意二元的乘积等于第三元, 所以上面 5 个一对一的映射都是同构. 因此有五个外同构.

2. n 元群如果它的中心是零, 那末它有 n 个互异的内同构, 因为 S_3 的中心是零, 所以它有六个内同构.

再因为同构把 n 阶元仍然变为 n 阶元, 所以任一自同构把(1 2), (1 3), (2 3) 互换, 二个不同的自同构有不同的互换, 于是 S_3 最多只能有六个自同构, 所以它没有外同构.

3. 因为命 $\pm 1 = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\pm i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\pm j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\pm k =$

$\pm\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$时，§2·3习题7中各关系式成立。

4. 因为$H\cap K$是G的子群，$H\cap K\subseteq K$，所以$H\cap K$是K的子群。再如果$a\in H\cap K$，$k\in K$，那末$kak^{-1}\in H$，$kak^{-1}\in K$，所以$kak^{-1}\in H\cap K$。

5. 因为$\bar{g}\bar{k}\bar{g}^{-1}=\bar{k}'$，即$\overline{gkg^{-1}}=\bar{k}'$，所以$gkg^{-1}=k'h$，因此$gkg^{-1}\subseteq K$。

6. 由群方程$p^n=a_0+a_1p+a_2p^2+\cdots$，得知$a_0\neq 1$。

7. 假如G的中心C的元数是p，命a是G中而不是C中的元，那末G所有与a能够交换的元形成的群就是G，因此$a\in C$，这与假设不合。

8. 假定$\sigma_a(x)=axa^{-1}$，如果$\sigma_a=\sigma_b$，那末$b^{-1}ax=xb^{-1}a$，因为G的中心是单位元群，所以$b^{-1}a=e$，于是$a=b$。

9. 假如c是中心C中任一元，g是G中任一元，如果$c\to c'$，$g'\to g$，因为$g'c=cg'$，所以$gc'=c'g$于是$c'\in C$。

10. 由$A\supseteq B\supseteq C$及σ是A的自同构，得$\sigma(B)\subseteq B$，如果$\sigma(B)\subset B$，命$b'\in B$但$\notin\sigma(B)$，b'的象源是b，显然$b\notin B$。所以σ^{-1}把$b'\to b$，这与B是特征子群的假设不合。于是$\sigma(B)=B$。因此σ又是B的自同构，所以$\sigma(c)\subseteq C$。

11. 因为$H\supseteq G'$，$ghg^{-1}h^{-1}\in H$，所以$ghg^{-1}\in H$，即$gHg^{-1}\subseteq H$。

13. 因为$S_4=A_4\cup(1\,2)A_4=H\cup(1\,2\,3)H\cup(1\,3\,2)H\cup(1\,4\,2)H\cup(1\,2)H\cup(2\,3)H\cup(1\,3)H\cup(1\,4)H$，而$(1\,2\,3)$，$(1\,3\,2)$，$(1\,4\,2)$，$(1\,2)$，$(2\,3)$，$(1\,3)$，$(2\,4)$中只有$(2\,3)$能够与$H$交换，所以$H$的正规化群$K=H\cup(2\,3)H$。再因为$S_4=K\cup(1\,2\,3)K\cup(1\,3\,2)K\cup(1\,4\,2)K$，于是它的共轭子群是

$$H=\{(1),(2\,3\,4),(2\,4\,3)\},\ (1\,2\,3)H(1\,3\,2)=\{(1),(1\,4\,3),(1\,3\,4)\},$$

$$(1\,3\,2)H(1\,2\,3)=\{(1),(1\,2\,4),(1\,4\,2)\},$$

$$(1\,4\,2)H(1\,2\,4)=\{(1),(1\,3\,2),(1\,2\,3)\}.$$

习题 2.5

1. 因为$S_4=A_4\cup(1\,2)A_4$，$A_4=B_4\cup(1\,2\,3)B_4\cup(1\,3\,2)B_4$，所以$S_4=B_4\cup(1\,2)B_4\cup(1\,3)B_4\cup(2\,3)B_4\cup(1\,2\,3)B_4\cup(1\,3\,2)B_4$。因此$S_4/B_4\cong\{(1),(1\,2),(1\,3),(2\,3),(1\,2\,3),(1\,3\,2)\}$。

3. 假定$\sigma_a(g)=aga^{-1}$，如果$\sigma_a=1$，那末$aga^{-1}=g$，即$ag=ga$，所以$a\in C$。因此同态核是C。

5. 假定$G\sim G'$，同态核是E，H'是G'的子群，H是H'在G的完全象

源，于是 $H' \cong H/E$.

6．$a \to a^{-1}$ 是逆同构映射．

习　题　3.1

1．分配律不成立．

2．成环，(1, 1) 是单位元，(0, 0) 是零元，$(a, 0)$，$(0, b)$ 都是零因子，(a, b) 的逆元是 (a^{-1}, b^{-1})．

5．假如 $ab=0$，$b\neq 0$ 时，如果有 a_L^{-1}，那末 $a_L^{-1}ab=b=0$．此不可．又假如有 a_R^{-1}，因为 $aa_R^{-1}+ab=a(a_R^{-1}+b)=e$，所以 $a_R^{-1}+b$ 又是 a 的右逆．再假如 $ab=e$，那末 $aba=ea=ae$，于是 $a(ba-e)=0$，如果 a 只有一个右逆元，因为它不是左零因子，所以 $ba=e$．

6．因为 $(r-re)a=0$．

8．假定 E_{ij} 是 i 行 j 列的元是 1，其余元都是 0 的方阵，因为 $(a_{ij})E_{ij}=E_{ij}(a_{ij})$，所以 $\begin{pmatrix} \vdots & a_{1i} & \vdots \\ & \vdots & \\ \vdots & a_{ni} & \vdots \end{pmatrix}=\begin{pmatrix} \cdots\cdots\cdots \\ a_{j1} \cdots a_{jn} \\ \cdots\cdots\cdots \end{pmatrix}$，于是 $a_{ki}=a_{jk}=0$，$a_{ii}=a_{jj}=a$，因此 $(a_{ij})=(a)$．

9．假如 $a^2=a$，$r\in R$．因为 $(ara-ar)^2=0$，所以 $ara=ar$．同样 $ara=ra$，于是 $ar=ra$．

10．由 $4a^2=2a$，我们有 $2a=0$，即 $a=-a$．又由 $(a+b)^2=a+b$，得 $ab+ba=0$，所以 $ab=ba$．

习　题　3.2

1．$Z-(2)$．

2．譬如 2，3 都是 $Z-(6)$ 的零因子．

3．假如 $c_1k=kc_1$，$c_2k=kc_2$，那末 $(c_1-c_2)k=k(c_1-c_2)$，$c_1^{-1}k=kc_1^{-1}$．

4．因为适当取 $(ae-bi-cj-dk)(ae+bi+cj+dk)=(a^2+b^2+c^2+d^2)e$ 中的复数 a，b，c，d 可使 $a^2+b^2+c^2+d^2=0$，所以这时 $ae+bi+cj+dk$ 是右零因子．

习　题　3.3

1．因为 R 是加群，$R\sim S$，所以 S 也是加群．再 S 中结合律，分配律可

以与§2.5定理1的证明类似证明、所以 S 成环．又因为乘群的同态象仍然是乘群，所以当 R 是体时，S 也是体．

3．如果同构，那末 $0\rightarrow e$．设 $a\rightarrow -e$，于是 $2a\rightarrow e$，所以 $2a=0$，因此 $2e=0$．再设 $e\rightarrow b$，那末 $b^2=e$，因为 $b^2-e^2=(b-e)(b+e)=0$，所以 $b=e$，即 $e\rightarrow e$，此不可．

6．因为 $e\rightarrow\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$，$i\rightarrow\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}$，$j\rightarrow\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$，$k\rightarrow\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$，即

$$ae+bi+cj+dk\rightarrow\begin{pmatrix}a+bi & c+di\\ -c+di & a-bi\end{pmatrix}$$

是同构映射，所以它们形成体．

习　题　3.4

1．有理数体包含这整环，而有理数体是质体，所以它的商体是有理数体．

3．$0+1$ 是单位元，所有形状象 $a+0$ 的元形成与 R 同构的环，所有形状象 $0+m$ 的元形成与 Z 同构的环．

习　题　3.5

1．当 R 是无零因子环时，m 次多项式与 n 次多项式的乘积就是 $m+n$ 次多项式．

3．$q(x)=\begin{pmatrix}2 & 0\\ 2 & 0\end{pmatrix}x-\begin{pmatrix}2 & 4\\ 2 & 4\end{pmatrix}$，$r=\begin{pmatrix}-5 & -11\\ -2 & 5\end{pmatrix}$；

$$q_0(x)=\begin{pmatrix}2 & 0\\ 2 & 0\end{pmatrix}x-\begin{pmatrix}6 & 0\\ -2 & 0\end{pmatrix},\quad r_0=\begin{pmatrix}-1 & 1\\ 14 & 1\end{pmatrix}.$$

习　题　3.6

1．所有形状象 $4r$ 的整数在整数环中形成主理想子环(4)，但在偶数环中形成的不是主理想子环(4)而是(8)．

5．在 $Z[x]$ 中，假如 $(x, 2)=(f(x))$，那末 $x=rf(x)$，$2=sf(x)$．于是 $f(x)=2$，因此 $r=\frac{1}{2}x\in Z[x]$．在 $Q[x]$ 中，$(x, 2)=(2)$．

6．因为 $f(x)=(x^2+1)q(x)+a+bx$，$\bar{f}(x)=\bar{a}+\bar{b}x$，所以 $a+bi\rightarrow\bar{a}+\bar{b}x$ 是它们的同构映射．

7. 因为 $S\sim S'$ 的同态核 $M\subseteq S$，又 $M\subseteq N$，所以 $M\subseteq S\cap N=0$.

8. 假定 $\bar{A}$ 是 $Z-(p^m)$ 中非零理想子环，$\bar{0}\neq\bar{a}\in\bar{A}$，那末 $a\not\equiv 0(p^m)$，但 $(a, p^m)=p^l$，$l<m$，所以 $p^l=ra+sp^m$，因此 $\bar{p}^l=\bar{r}\bar{a}+\bar{s}\bar{p}^m=\bar{r}\bar{a}\in\bar{A}$.

9. 假定 R 中所有形状象 ra^n，$r\in R$，的元形成的理想子环是 A_n，因为 $A_1, A_2, \cdots, A_n, \cdots$ 中必有相同的，命 $A_m=A_n$，$m<n$，那末 $ba^m=ra^n$，于是 $b=a(ra^{n-m-1})$，因此 $ax=b$ 在 R 中有解.

10. 假定 R 有单位元 1，那末中心 $C\neq 0$. 命 $c\in C$，因为 Rc 是 R 的理想子环，并且 $Rc\neq 0$，所以 $Rc=R$，因此 $c'c=1$ 即 $c'=c^{-1}$. 又因为 $c'r=c'r\cdot 1=c'r\cdot cc'=c'c\cdot rc'=rc'$. 所以 $c'\in C$.

再假如 R 的中心 $C\neq 0$. 命 $c\in C$，因为 $Rc=cR$，如果 $Rc=0$，那末 (c) 就是 R 中异于零的理想子环. 于是 $(c)=R$，这与 R 不是幂零环的假设不合. 所以 $Rc=R$，因此 $ec=ce=c$. 如果 $rc=b$，那末 $eb=erc=ecr=cr=b$. 所以 e 是 R 的单位元.

习 题 3.7

1. $(6):(3)=(2)$，$(6):(5)=(6)$，$(3):(9)=R$.

3. (i)→(iii)，$A:BC=(A:B):C=A:C=A$. (iii)→(ii)，因为 $BC\subseteq B\cap C$，所以 $A:(B\cap C)\subseteq A:BC=A$. 因此 $A:(B\cap C)=A$. (ii)→(i)，因为 $B\cap C\subseteq B$，所以 $A:B\subseteq A:(B\cap C)=A$，因此 $A:B=A$.

6. 因为 $(A, B)=R$ 时，$AB=A\cap B$，再因为 $(A, B)=R$，$(A, C)=R$ 时，$(A, BC)=R$，所以 $ABC=A\cap BC=A\cap B\cap C$.

习 题 3.8

1. 因为 $Q[x]-(x)\simeq Q$，所以 (x) 是无零因子环.

2. 因为 $Z[x]-(x)\simeq Z$，所以 (x) 是质理想子环. 又因为 $Z[x]-(2, x)\simeq Z-(2)$，所以 $(2, x)$ 是极大理想子环.

3. 假定 $(a+bi)(c+di)\equiv 0(3)$，那末 $(a^2+b^2)(c^2+d^2)\equiv 0(3)$，但当 $a^2+b^2\equiv 0(3)$ 时 $a\equiv 0$，$b\equiv 0$，因为 $a\not\equiv 0$ 时 $a^2\equiv 1$. 所以 (3) 是质理想子环.

又因为 $2=(1-i)(1+i)\equiv 0(1+i)$，$1-i=(1+i)(-i)\equiv 0(1+i)$，所以 $a+bi\equiv a+b\equiv 0$ 或 1. 于是 $Z[i]-(1+i)=\{\bar{0}, \bar{1}\}\simeq Z-(2)$，因此 $(1+i)$ 是极大理想子环.

5. 因为 $P\neq A$，所以 $P\subset A$. 命 $p\in P$，$a\in A$，$a\bar{\in}P$，r 是 R 中任一元，

因为 $ra\in A$，所以 $ra\cdot p=a\cdot rp\in P$，因此 $rp\in P$。

6．假定 N 是 R 的极大理想子环，如果 $a\overline{\in}N$，$b\overline{\in}N$，那末 $(N,a)=R$，$(N,b)=R$，于是 $(N,a)(N,b)=(N,ab)=R$，所以 $ab\overline{\in}N$。

7．必要条件由定理 1 的充分条件证法即得．充分条件用定理 1 的必要条件的证法，其中以 ar 形成的理想子环 A 代替 (a)，因为 $\bar{a}\neq 0$，所以 $a^2\not\equiv 0$ (N)，于是 $N\subset(A,N)$，因此 $(A,N)=R$。

8．因为 $R\sim\bar{R}=R-N$．如果 A 是 R 包含 N 的理想子环，$R\supset A\supset N$，那末 A 在 $\bar{R}$ 中的象集 $\bar{A}$ 是 $\bar{R}$ 中非零的理想子环．反过来，如果 $\bar{A}$ 是 $\bar{R}$ 中非零的理想子环，那末 $\bar{A}$ 在 R 中的完全象源 A 是 R 的理想子环。

习 题 3.9

1．因为 $Z-(19)$ 成体，所 $6x\equiv 17(19)$ 有解．显然 $x=6$ 是它的解．

2．假如 $(a+b\sqrt{-5})(c+d\sqrt{-5})=3$ 或 $2+\sqrt{-5}$，那末

$$(a^2+5b^2)(c^2+5d^2)=9,$$

于是
$$\begin{cases}a^2+5b^2=3\\ c^2+5d^2=3\end{cases}\quad 或\quad \begin{cases}a^2+5b^2=9\\ c^2+5d^2=1,\end{cases}$$

前者不可能，后者 $c=1$，$d=0$，因此 $c+d\sqrt{-5}=1$ 是单位元．

3．因为 b，c 与 a 无公约时，bc 也与 a 无公约．又当 b 与 a 无公约时，$ra+sb=1$．于是 $\bar{r}\bar{a}+\bar{s}\bar{b}=\bar{1}$，所以 $\bar{s}\bar{b}=\bar{1}$．

4．假定对于 $\alpha=a+bi$，命 $\sigma(\alpha)=a^2+b^2$．$\beta=c+di$，适当取 $\alpha-\delta\beta$ 中的 δ 使 $\sigma(\alpha-\delta\beta)<\sigma(\beta)$．但 $\sigma(\alpha-\delta\beta)=\sigma\left(\beta\cdot\left(\frac{\alpha}{\beta}-\delta\right)\right)=\sigma(\beta)\sigma\left(\frac{\alpha}{\beta}-\delta\right)$，因此取适合 $\sigma\left(\frac{\alpha}{\beta}-\delta\right)<1$ 的 δ 即可．因为

$$\frac{\alpha}{\beta}=\frac{(a+bi)(c-di)}{c^2+d^2}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i,$$

如果 $\delta=u+vi$，那末

$$\frac{\alpha}{\beta}-\delta=\left(\frac{ac+bd}{c^2+d^2}-u\right)+\left(\frac{bc-ad}{c^2+d^2}-v\right)i.$$

取适合
$$\left|\frac{ac+bd}{c^2+d^2}-u\right|\leqslant\frac{1}{2},\quad\left|\frac{bc-ad}{c^2+d^2}-v\right|\leqslant\frac{1}{2}$$

的整数 u，v 即得 $\sigma\left(\frac{\alpha}{\beta}-\delta\right)\leqslant\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$．

5．假定 $f(x)=\sum a_ix^i$，$g(x)=\sum b_jx^j$，$f(x)g(x)=\sum c_\lambda x^\lambda$，$c_\lambda=\sum\limits_{i+j=\lambda}a_ib_j$，

因为 a_i 没有公因数，b_j 也没有公因数，命 a_i 中第一个不能用质数 p 整除的是 a_k，b_j 中第一个不能用 p 整除的是 b_l，于是 c_{k+l} 就不能用 p 整除，所以 c_λ 没有公因数。

习 题 3.10

1. 在 R 中只有一个零点 1.

习 题 4.2

1. 因为质体是所有子体的交集，所以它在中心里面.

2. $2=(1-i)(1+i)\equiv 0(1+i)$，所以特征数是 2.

4. 假定 P 是 K 的质体，因为 x^p-x 在 K 中的零点不多于 p 个，而 P 中 p 个元都是它的零点，所以 $K=P$.

5. 因为 $2a=(2a)^2=4a^2=4a$，所以 $2a=0$. 又因为 $a+b=(a+b)^2=a^2+ab+ba+b^2=a+ab+ba+b$，所以 $ab+ba=0$，于是 $ab+2ba=ba$，即 $ab=ba$.

习 题 4.3

1. $\dfrac{1-7\alpha+2\alpha^2}{1+\alpha-\alpha^2}=\dfrac{3\alpha-13}{-4(\alpha-2)}=\dfrac{(3\alpha-13)(\alpha-3)}{-4(\alpha-2)(\alpha-3)}=-\dfrac{1}{4}(-7\alpha+18)$.

2. $-1+\sqrt[3]{2}$.

3. 因为 i 适合既约多项式 x^2-1，所以 $F(i)\cong F[x]/(x^2+1)$.

4. 因为 $\alpha=\dfrac{-1+\sqrt{3}i}{2}$，所以 $F(\alpha)=F(i)$，即 $F(\alpha)$ 是复数体.

5. $K(\alpha)=K(x^{\frac{1}{p}})=F(x^{\frac{1}{p}})=F(\alpha)$，$z^p-x=(z-\alpha)^p$.

6. 因为 $F[x]\sim F[\alpha]$，$f(\alpha)=0$，所以 $f(x)\equiv 0(p(x))$.

7. 因为 $\dfrac{1}{\alpha}\in F[\alpha]$，所以 $\dfrac{1}{\alpha}=f(\alpha)$，即 $\alpha f(\alpha)=1$.

习 题 4.4

2. $(Q(i,\sqrt{2}):Q)=4$.

4. p^n.

6. 假如 $\sqrt{b}=m+n\sqrt{a}$，那末 $b=m^2+n^2a+2mn\sqrt{a}$，首先 $mn=0$，因为不如此，b 不是整数. 再 $n\neq 0$，因为不如此，b 有相同的质因数. 于是

$m=0$, 因此 $b=n^2a$. 假定 $n=\frac{r}{s}$, 那末 $s^2b=r^2a$. 于是 $r^2|b$, $s^2|a$, 所以 $r=1, s=1$. 因此 $b=a$.

7. 因为环的中心是环,所以 F 的代数的中心 C 是环. 再假如 $u\in C$, $a\in F$,显然 $au\in C$.

8. 假定 $A=Fu_1+\cdots+Fu_n$, $\alpha\neq0$, $\beta\in A$,因为 A 是无零因子环, $u_1, \cdots, u_n$ 是它的底,所以 $\alpha u_1, \cdots, \alpha u_n$ 也是它的底, 于是 $\beta=\sum a_i\alpha u_i=\alpha\sum a_iu_i$,所以 $\alpha x=\beta$ 在 A 中有解.

习 题 4.5

1. 假定 $a_0\alpha^n+\cdots+a_{n-1}\alpha+a_n=0$ 中 $a_n\neq0$, 那末 $\alpha\cdot\{-a_n^{-1}\beta(a_0\alpha^{n-1}+\cdots+a_{n-1})\}=\beta$, 如果 $a_n=0$, 那末 $a_0\alpha^{n-1}+\cdots+a_{n-1}=0$.

习 题 4.6

1. 因为 $x^3-x^2-x-2=(x-2)(x^2+x+1)$,所以分裂体是 $Z(\sqrt{-3})$.

2. 因为 $x^4+4x^2+2=(x^2+2-\sqrt{2})(x^2+2+\sqrt{2})$, 所以它的零点是 $\pm\sqrt{2-\sqrt{2}}\,i$, $\pm\sqrt{2+\sqrt{2}}\,i$. 又因为 $\sqrt{2}\in K=Z(\sqrt{2-\sqrt{2}}\,i)$, 所以

$$\sqrt{2+\sqrt{2}}\,i=-\frac{\sqrt{2}}{\sqrt{2-\sqrt{2}}\,i}\in K.$$

3. 因为 $(F(\alpha):F)=2$,所以 α 满足的既约多项式 $f(x)$ 的次数是 2. 因此 $F(\alpha)$ 是 $f(x)$ 的分裂体.

5. 因为 K 中任意元是在添加有穷个多项式的零点于 F 的体中.

6. 因为 3 次多项式 $f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ 的判别式 $D=\{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\}^2>0$ 时, $\alpha_1, \alpha_2, \alpha_3$ 是 3 个不同的实根,又因为

$$(x-\alpha_2)(x-\alpha_3)=x^2-(\alpha_2+\alpha_3)x+\alpha_2\alpha_3\in Z(\alpha_1)[x],$$

所以 $$\alpha_2+\alpha_3,\ \alpha_2\alpha_3,\quad (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\in Z(\alpha_1).$$

假如 $\sqrt{D}\in Z$, 那末 $\alpha_2-\alpha_3=\sqrt{D}/(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\in Z(\alpha_1)$, 因此 α_2, $\alpha_3\in Z(\alpha_1)$,所以 $f(x)$ 是 Z 的正规式.

假如 α_2, $\alpha_3\in Z(\alpha_1)$, 那末 $\sqrt{D}=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)=a\in Z(\alpha_1)$, 如果 $a\notin Z$, 那末 $(Z(a):Z)=2$, 这与 $(Z(\alpha_1):Z)=3$ 的性质矛盾. 所以 $a\in Z$, 即 D 是有理数的平方.

习　题　4.7

1．因为 $x^{\frac{1}{p}} \notin F(x)$，所以 $y^p - x = (y - x^{\frac{1}{p}})^p$ 在 $F(x)[y]$ 中是既约。

3．假定 $\alpha_1, \cdots, \alpha_n$ 是 $f(x)$ 的零点，因为 $\alpha_i^p - \alpha_j^p = (\alpha_i - \alpha_j)^p \neq 0$，而

$$g(\alpha_k^p) = \sum a_i^p \alpha_k^{ip} = (\sum a_i \alpha_k^i)^p = 0,$$

所以 $\alpha_1^p, \cdots, \alpha_n^p$ 是 $g(x)$ 的 n 个互异零点．如果 $h(x)$ 是 $F[x]$ 中 $g(x)$ 的既约因式，$h(\alpha_k^p)=0$，于是 $h(x^p)$ 与 $f(x)$ 有公共零点 α_k，所以 $f(x) \mid h(x^p)$，于是 $h(\alpha_i^p)=0$，$i=1, \cdots, n$．因此 $g(x)=h(x)$，即 $g(x)$ 是可离多项式．

4．假如 F 是完全体，因为 $x^p - a = (x - a^{\frac{1}{p}})^p$ 有重零点，所以它在 $F[x]$ 中不是既约，于是 $x - a^{\frac{1}{p}} \in F[x]$，即 $a^{\frac{1}{p}} \in F$．反过来，假如 F 中任意元的 p 乘根都在 F 中，因为 x^p 的任意多项式

$$f(x) = \sum a_i x^{ip} = (\sum a_i^{\frac{1}{p}} x^i)^p$$

都不是既约，所以 $F[x]$ 中的既约多项式都是可离多项式．

5．假如 K 是完全体 F 的代数体，K 的代数元 α 适合既约多项式 $f(x) = \sum a_i x^i$，显然 α^p 是既约多项式 $g(x) = \sum a_i^p x^i$ 的零点，于是 $F(\alpha) = F(\alpha^p)$．所以 $\alpha = \sum b_i \alpha^{ip} = (\sum b_i^{\frac{1}{p}} \alpha^i)^p$，即 $\alpha^{\frac{1}{p}} \in F(\alpha)$，因此 K 是完全体．

再假如 K 是不完全体 F 的 n 次扩张体，$u_1, \cdots, u_n$ 是 K 关于 F 的底，显然 $u_1^p, \cdots, u_n^p$ 是 K^p 关于 F^p 的底．于是 $(K:F) = (K^p:F^p)$．如果 $K = K^p$，那末 $F = F^p$，这与 F 是不完全体的假设不合．因此 $K \supset K^p$．所以 K 是不完全体．

6．假定 K 中元 α 的指数是 k，因为 $x^{p^k} - \alpha^{p^k} = (x - \alpha)^{p^k}$ 在 $F[x]$ 中是既约的，所以 K 是 F 的正规体．又假定 $\alpha \to \alpha'$ 是 K 关于 F 的同值映射，因为 $\alpha^{p^k} \in F$，所以 $\alpha'^{p^k} \in F$，于是 $\alpha^{p^k} = \alpha'^{p^k}$，因此 $\alpha = \alpha'$．所以 K 关于 F 的同值映射是恒等映射．

7．假定 β 是 $F(\alpha)$ 中关于 F 的可离元，那末 $F(\beta)$ 有 $(F(\beta):F)$ 个关于 F 的同值映射，把这些映射延长就得到 $F(\alpha)$ 关于 F 的同值映射．但这时 $F(\alpha)$ 关于 F 的同值映射，显然只有 1 个恒等映射，因此 $F(\beta) = F$，即 $\beta \in F$．所以 $F(\alpha)$ 是 F 的纯不可离体．

8．因为 K 关于 F 的缩减次数是 K 关于 F 的互异同值映射的个数．

习　题　4.8

1．$\sqrt{3} + \sqrt[3]{2}$．

2. $\sqrt{2}i$.

3. $(F(x^{\frac{1}{p}}, y^{\frac{1}{p}}):F(x, y))=p^2$,即 $n=p^2$, 但这时 $e=1$.

习 题 4.9

1. 因为 $Z/(p)$ 是元数为 p 的有穷体,所以对于任意 $a\not\equiv 0(p)$,有 $a^{p-1}\equiv 1(p)$.

2. 因为 $f(x)=\sum\limits_{i=0}^{m}a_ix^i$. $a_i^p=a_i$,所以 $f(\alpha^p)=\sum a_i^p\alpha^{ip}=(\sum a_i\alpha^i)^p=0$, 即 α^p 是 $f(x)$的零点. 同样 α^{p^2}, $\cdots$, α^{p^m} 都是 $f(x)$的零点. 因为$(F(\alpha):F)=m$, 所以 $F(\alpha)=GF(p^m)$, 因此 $\alpha^{p^m}=\alpha$.

3. 假定 $\alpha\in GF(p^n)$,那末 $\alpha^{p^n}=\alpha$,即$(\alpha^{p^{n-1}})^p=\alpha$,所以 $\alpha^{p^{n-1}}$ 是 α 的 p 次根. 于是任意 x^p 的多项式都是某个多项式的 p 次幂,因此任意 x^p 的多项式都不是既约的.

4. 假如 $a^{\frac{1}{p}}=x$, $a^{\frac{1}{p}}=y$,那末 $a=x^p=y^p$,于是 $(x-y)^p=0$, 所以 $x=y$.

5. 因为 h 次单位根得由 h 次本原单位根的乘幂而成.

6. 假定 F 是 $K=GF(3^2)$的质体, 因为 K 是 $f(x)=x^9-x=(x^4+1)(x^2+1)(x^2-1)x$ 的分裂体, $g(x)=x^2+1$ 在 $F[x]$中是既约的,如果 i 是 $g(x)$在 K 中的零点, 那末 $K=F(i)$, 因此 K 中任意元可以写成 $a+bi$ 形状. 又因为 $1+i$ 是 K 中阶是 8 的元,所以 K 的乘群 $K^*=(1+i)$.

习 题 4.10

1. 假定 $u_1, \cdots, u_m$ 是 K 关于 L 的代数底, $v_1, \cdots, v_n$ 是 L 关于 F 的代数底,那末 $M=\{u_1, \cdots, u_m, v_1, \cdots, v_n\}$关于 F 代数无关,这是因为如果 u_1 与 $M-u_1$ 或 v_1 与 $M-v_1$ 关于 F 代数相关, 显然$\{u_1, \cdots, u_m\}$关于 L 代数相关, 这与假设不合. 再因为$\{u_1, \cdots, u_m\}$是 K 关于 L 的代数底,所以 K 是 $L(u_1, \cdots, u_m)$的代数体. 又因为 L 是 $F(v_1, \cdots, v_n)$的代数体,所以 $L(u_1, \cdots, u_m)$ 是 $F(M)$的代数体, 因此 K 是 $F(M)$的代数体. 于是 K 中任意元关于 F 与 M 代数相关. 所以 M 是 K 关于 F 的代数底.

2. 因为 $F(u, v)\supset F(u, v^2+u)\supset F(u^3+v^2, v^2+u)$.

3. $F(x)$关于 F 的任一自同构是把 x 变为 $F(x)$的本原元 $u=\dfrac{ax+b}{cx+d}$, $ad-bc\neq 0$.

习 题 5.1

1．因为同态把子群 H 变为子群 H'．假如 $h'\in H'$，由 $h\to h'$ 有 $\lambda h\to\lambda h'$，但 $\lambda h\in H$，所以 $\lambda h'\in H'$，因此 H' 是带算子群．

2．假如 $G=(a)$，$\lambda a=a^k$，$H=(a^m)$，那末 $\lambda a^m=(\lambda a)^m=(a^m)^k\in H$．

3．因为 $(a,\ 0)\to(0,\ a)$ 时 $(a,\ 0)(b,\ 0)$ 与 $(0,\ a)(0,\ b)$ 对应，但 $(\lambda_1,\ \lambda_2)(a,\ 0)=(\lambda_1 a,\ 0)$，$(\lambda_1,\ \lambda_2)(0,\ a)=(0,\ \lambda_2 a)$，所以 $(\lambda_1,\ \lambda_2)(a,0)$ 不与 $(\lambda_1,\ \lambda_2)(0,\ a)$ 对应．

习 题 5.2

1．因为 $S_4=S_3B_4$，而 $S_3\cap B_4=(1)$，所以 $S_4/B_4\cong S_3$．

2．因为 $S_n=G\cdot A_n$，所以 $S_n/A_n=G\cdot A_n/A_n\simeq G/G\cap A_n=G/H$．

3．由第二同构定理，$H\cap K/H\cap K'\simeq K'(K\cap H)/K'\subseteq K/K'$．

5．$F(\alpha)\cong\{Z-(p)\}[x]-A$，因 $Z\sim Z-(p)$，所以 $Z[x]\sim\{Z-(p)\}[x]$，假如 A 在 $Z[x]$ 的完全象源是 N，那末 $\{Z-(p)\}[x]-A\cong Z[x]-N$，因此 $F(\alpha)\cong Z[x]-N$．

习 题 5.3

1．S_2 是可换群，$S_3\supset A_3\supset 1$ 的商群列的元数是 2，3，所以都是可解群．

2．因为 $G/H=\bar{G}$，H 都是可解群，所以它们有商群是可换群的正规群列 $\bar{G}_0\supset\bar{G}_1\supset\cdots\supset\bar{G}_m=\bar{E}$，$H=H_0\supset H_1\supset\cdots\supset H_n=E$．命 G_i 是 $\bar{G}_i$ 在 G 中的完全象源，那末 $G=G_0\supset G_1\supset\cdots\supset G_m=H=H_0\supset H_1\supset\cdots\supset H_n=E$．

6．S_4 的所有合成群列为 $S_4\supset A_4\supset B_4\supset C_i\supset E$，这里

$$C_1=\{(1),\ (1\,2)(3\,4)\},\quad C_2=\{(1),\ (1\,3)(2\,4)\},$$
$$C_3=\{(1),\ (1\,4)(2\,3)\}.$$

7．无穷可换群的极大子群仍然是无穷群．

8．因为 $Q(\sqrt[4]{2},\ i)\supset Q(\sqrt[4]{2})\supset Q(\sqrt{2})\supset Q$ 是 $Q(\sqrt[4]{2},\ i)$ 的合成体列．

习 题 5.4

1．由 $ur+vs=1$ 得 $a=(a^r)^u\cdot(a^s)^v$，因此 $(a)=(a^r)\cdot(a^s)$．再命 $b\in(a^r)$

$\cap(a^s)$，那末 $b=a^{sh}=a^{rk}$，于是 $sh\equiv rk(n)$，即 $sh-rk=mn=mrs$，因此 $sh=r(k+ms)$，所以 $r|h$，因此 $b=e$，即 $(a^r)\cap(a^s)=e$。

3．假如 $A=\{e, a, a^2\}$，$B=\{e, b, b^2\}$，那末

$$A\times B=\{e, a, a^2, b, ab, a^2b, b^2, ab^2, a^2b^2\}.$$

4．假设 $G/H=(\bar{a})$，$K=(e)$，显然 $K\cong G/H$，并且 $G=HK$。

5．因为 $G=AB$，所以 $g=ab$，于是 $\bar{g}=\bar{a}\bar{b}$，因此 $\bar{G}=\bar{A}\bar{B}$。再 $\bar{A}$，$\bar{B}$ 都是 $\bar{G}$ 的正规子群，假如 $c\in\bar{A}\cap\bar{B}$，那末 $c\in A\cap B=H$，因此 $\bar{c}=\bar{e}$，即 $\bar{A}\cap\bar{B}=e$。

6．因为 $A\times B$ 的长 $=A$ 的长 $+B$ 的长，$\bar{G}=G/H$ 时，G 的长 $=\bar{G}$ 的长 $+H$ 的长．

8．假定 $c\in C$，$c=a_1+\cdots+a_n$，$a_i\in R_i$，对于 R_i 中任一元 r_i，因为 $R_iR_j=0$，$i\neq j$，所以 $cr_i=a_1r_i+\cdots+a_nr_i=a_ir_i$，于是 $a_i\in C_i$，因此 C 是 C_1，$\cdots$，C_n 的和，再因为 R 是 R_1，$\cdots$，R_n 的直和，所以 $c=a_1+\cdots+a_n$ 的表示是一意的．

9．因为 $ee_j=e_j=e_1e_j+\cdots+e_je_j+\cdots+e_ne_j=\sum\limits_{i=1}^{n}e_ie_j$，所以 $e_ie_j=0$，$i\neq j$，$ee_i=e_i=e_i^2$。反过来，假如 $e=e_1+\cdots+e_n$，$e_ie_j=0$，$i\neq j$，$e_i^2=e_i$，那末 $r=re=re_1+\cdots+re_n$，即 R 是 $L_1=Re_1$，$\cdots$，$L_n=Re_n$ 的和．再当 $r_1e_1+\cdots+r_ne_n=0$，两边用 e_i 右乘即得 $r_ie_i=0$，所以这表示又是一意的．因此 R 是 L_1，$\cdots$，L_n 的直和．

10．假定 e 是 R 的幂等元，但不是单位元，那末 R 中所有满足 $r_1e=er_1=r_1$ 的元 r_1 形成理想子环 R_1，显然 e_1 是 R_1 的单位元。

习　题　5 5

1．循环群与非循环群两类．前者是 2 元群与 9 元循环群的直积，后者是 2 元群与两个 3 元群的直积．

2．假定 $G=(a)$ 的元数 $n=pq$，$(p, q)=1$．因为 G 中任意元的阶都是 n 的约数，所以 n 是它们的公倍数．但 a^p 的阶是 q，a^q 的阶是 p，所以 n 是它们的最小公倍．反过来，由 §2.2 习题 5，G 中有阶为 n 的元，因此 G 是循环群．

3．假定 $G=(a_1)\times(a_2)\times(a_3)\times(a_4)\times(a_5)$，它们的元数分别是 2^3，2^4，3，3^2，3^4．命 $G_1=(a_3)$，$G_2=(a_1)\times(a_4)=(a_1a_4)$，$G_3=(a_2)\times(a_5)=(a_2a_5)$，显然 $G=G_1\times G_2\times G_3$，这时 G_1，G_2，G_3 的元数分别是 3，$2^3\cdot3^2$，$2^4\cdot3^3$．

4．因为 $\chi_0(a)=e$，所以 $\sum\limits_{i=1}^{n}\chi_0(a_i)=ne$．又因为 $\chi(a_i)=\xi^{k_i}$，所以

$\sum_{i=1}^{n}\chi(a_i)=\sum_{i=1}^{n}\xi^{k_i}$. 但 ξ^{k_i} 是 $x^{n_i}=e$ 的零点，因此也是 $x^n=e$ 的零点，所以 $\sum_{i=1}^{n}\xi^{k_i}=0$。

习　题　5.6

1．把 G 就 G_a 分为陪集 $\tau_i G_a$，因为 G 是可迁群，所以这样的陪集有 m 个，如果 G_a 的元数是 q，那末 G 的元数 $n=mq$.

2．因为 $G_{\tau(a)}=\tau G_a\tau^{-1}$，所以 G_a 与 $G_{\tau(a)}$ 共轭．假如 G_a 中任意变换不使文字 b 变动，那末 $G_a\subseteq G_b$，但 G_a，G_b 的元数相等，因此 $G_a=G_b$，于是 $G_a=\tau G_a\tau^{-1}$，即 τ 与 G_a 能够交换．

4．H 的所有非原系为{1, 2}，{3, 4}，{5, 6}；{1, 3}，{2, 5}，{4, 6}；{1, 6}，{2, 4}，{3, 5} 及 {1, 4, 5}，{2, 3, 6}.

习　题　6.1

1．假定 $f(x)$ 是 $F[x]$ 中的 3 次既约多项式，如果 $f(x)$ 是正规式，那末 $(K:F)=3$，因此 $G=A_3$．如果 $f(x)$ 不是正规式，那末 $(K:F)=6$．因此 $G=S_3$.

2．因为 $\sqrt{D}=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)=d$，由 § 2.2 定理 3 的证明得知偶排列不使 d 变动，奇排列把 d 变为 $-d$．于是假如 G 是全由偶排列所成，那末 $d\in F$，即 D 的平方根在 F 中．反过来，假如 $d\in F$，那末 G 中任意元不使 d 变动．因此 G 是全由偶排列组成的．

3

	1	σ	τ	ρ
$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
i	i	$-i$	i	$-i$

	1	σ	τ	ρ
1	1	σ	τ	ρ
σ	σ	1	ρ	τ
τ	τ	ρ	1	σ
ρ	ρ	τ	σ	1

4．与由对于模 n 的既约同余系形成的乘群同构，因此是可换群．

5　由 § 4.6 习题 6，x^3-2，x^3+2x+1 都不是正规式，因此它们的伽罗瓦群都是 S_3.

又因为 $x^4-10x^2+1=(x^2-1)^2-8x^2=\{(x-\sqrt{2})^2-3\}\{(x+\sqrt{2})^2-3\}=(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})$，所以其分裂体 $K=Q(\sqrt{2}, \sqrt{3})$．于是其伽罗瓦群 $G=\{1, \sigma, \tau, \rho\}$ 的群

表为

	1	2	3	4
1	1	2	3	4
σ	2	1	4	3
τ	3	4	1	2
ρ	4	3	2	1

其中 $1=\sqrt{2}+\sqrt{3}$, $2=\sqrt{2}-\sqrt{3}$,

$3=-\sqrt{2}+\sqrt{3}$, $4=-\sqrt{2}-\sqrt{3}$.

6. 因为在 $Q[x]$ 中 x^4-10x^2+1 是既约而 x^4-5x^2+6 是可约，所以前者的伽罗瓦群是可迁群而后者的是非迁群.

又因为 $x^4-5x^2+6=(x^2-2)(x^2-3)=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})\cdot(x+\sqrt{3})$，它的伽罗瓦群 $G=\{1, \sigma, \tau, \rho\}$ 的群表为

	1	2	3	4
1	1	2	3	4
σ	2	1	3	4
τ	1	2	4	3
ρ	2	1	4	3

其中 $1=\sqrt{2}$, $2=-\sqrt{2}$,

$3=\sqrt{3}$, $4=-\sqrt{3}$.

7. 由定理 2, $K=F(\alpha)$, α 是多项式 x^p-a 的零点，的伽罗瓦群与 p 次单位根形成的 p 元循环群的子群同构，但 p 元循环群的子群只有自身及单位元群. 从前者言，x^p-a 在 $F[x]$ 中是既约，从后者言，x^p-a 在 $F[x]$ 中完全分裂.

8. 假如 $x^p-a=f(x)g(x)=h(x-\varepsilon^i\alpha)$, $\alpha^p=a$, 那末 $f(x)$ 中不含 x 的项 $\pm b$ 必为 $\pm\varepsilon^l\alpha^k$, 即 $b=\varepsilon^l\alpha^k$. 于是 $b^p=\alpha^{pk}=a^k$, $0<k<p$. 因此 $(k, p)=1$, 即 $rk+sp=1$. 所以

$$a=a^{rk}\cdot a^{sp}=b^{rp}\cdot a^{sp}=(b^r a^s)^p=\alpha^p,\quad \alpha=b^r a^s\in F,$$

于是 $$x^p-a=x^p-\alpha^p=(x-\alpha)(x^{p-1}+\alpha x^{p-2}+\cdots+\alpha^{p-1}).$$

习 题 6.2

1. 假定 (G_1, G_2) 所属的体是 K'，因为 $G_i\subseteq(G_1, G_2)$，所以 $K'\subseteq K(G_i)$，因此 $K'\subseteq K(G_1)\cap K(G_2)$. 再命 $\alpha\in K(G_1)\cap K(G_2)$，那末 G_1, G_2 中任意元不使 α 变动. 因此 (G_1, G_2) 中任意元也不使 α 变动. 于是 $\alpha\in K'$，即 $K(G_1)\cap K(G_2)\subseteq K'$. 因此 $K'=K(G_1)\cap K(G_2)$.

又假定 $G_1\cap G_2$ 所属的体是 K''，因为 $G_1\cap G_2\subseteq G_i$，所以 $K(G_1)$, $K(G_2)\subseteq K''$. 于是 $F(K(G_1), K(G_2))\subseteq K''$. 但 $F(K(G_1), K(G_2))$ 所属的群 G' 显然是 $G_1\cap G_2$ 的子群，即 $G'\subseteq G_1\cap G_2$，所以 $F(K(G_1), K(G_2))\supseteq K''$. 因此

$K''=F(K(G_1),\ K(G_2))$.

2．因为 $F(K_1,\ K_2)$ 所属的群 $G'\subseteqq G(K_1)\cap G(K_2)$。但 $G(K_1)\cap G(K_2)$ 所属的体是 $F(K_1,\ K_2)$，因此 $G'=G(K_1)\cap G(K_2)$。

又因为 $K_1\cap K_2$ 所属的群 $G''\supseteqq G(K_1)$，所以 $G''\supseteqq(G(K_1),\ G(K_2))$。但 $(G(K_1),\ G(K_2))$ 所属的体是 $K_1\cap K_2$，因此 $G''=(G(K_1),\ G(K_2))$。

3．因为 $F(\alpha)$ 是 F 的正规体，所以 $K(\alpha)$ 也是 K 的正规体。假如 $K(\alpha)$ 关于 K 的伽罗瓦群 G 与 $F(\alpha)$ 关于 F 的伽罗瓦群 G' 一致，因为 G 中任意元不使 K 中任意元变动，当然也不使 F 中任意元变动，并且 $F(\alpha)$ 中元对于 G 中任意元不变动的只有 F 中元，因此 $F(\alpha)\cap K=F$。

反过来，假如 $F(\alpha)\cap K=F$，那末 $F[x]$ 中 α 适合的既约多项式 $f(x)$ 也是 $K[x]$ 中 α 适合的既约多项式．因此 $f(x)$ 在 $F(\alpha)$ 中的零点 $\alpha_1=\alpha,\ \cdots,\ \alpha_n$ 也是 $f(x)$ 在 $F(\alpha)$ 中的零点．于是 $\alpha\to\alpha_i$ 是 G' 中元也是 G 中元，所以 G 与 G' 一致。

4．假定 $K\supseteqq K_1\supseteqq F$，$G(K_1)=G_1$，因为 G 是阿贝耳群，所以 G 的子群 G_1 是 G 的正规子群，因此 K_1 是 F 的正规体．

5．假定 L_i 是 K 中 L 的共轭子体，那末 $F(L,\ L_i,\ \cdots)$ 是 K 中包含 L 的 F 的最小正规体，于是 $F'=F(L,\ L_i,\ \cdots)$，因此它的伽罗瓦群 $G'=G(L)\cap G(L_i)\cap\cdots$.

6．K 的伽罗瓦群 G 是 8 元群，其元素为

	1	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

再因为 E，Q 的中间体中，关于 Q 是 2 次的有 3 个：$Q(i)$，$Q(\sqrt{2})$，$Q(i\sqrt{2})$，它们所属的群都是 4 元群，分别为

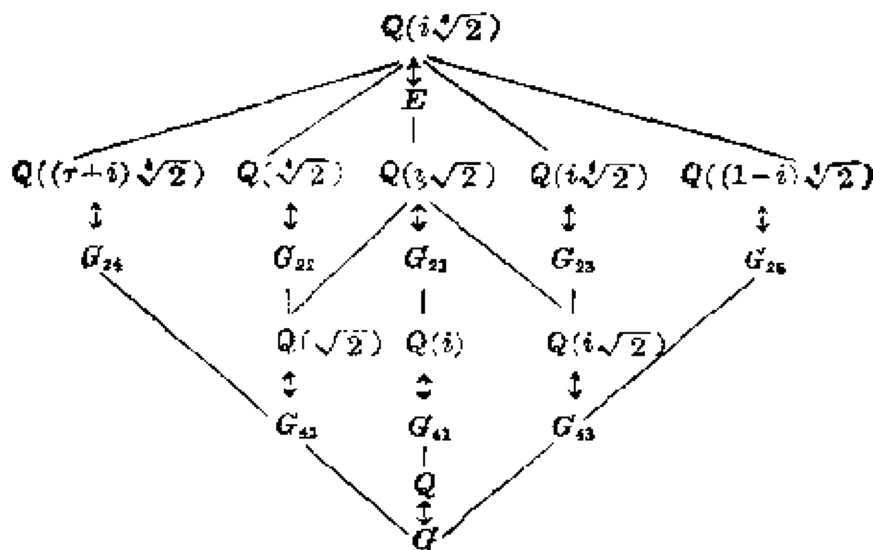
$G_{41}=\{1,\ \sigma,\ \sigma^2,\ \sigma^3\}$，$G_{42}=\{1,\ \sigma^2,\ \tau,\ \sigma^2\tau\}$，$G_{43}=\{1,\ \sigma^2,\ \sigma\tau,\ \sigma^3\tau\}$；

关于 Q 是 4 次的有 5 个：$Q(i,\sqrt{2})$，$Q(\sqrt[4]{2})$，$Q(i\sqrt[4]{2})$，$Q((1+i)\sqrt[4]{2})$，$Q((1-i)\sqrt[4]{2})$，它们所属的群都是 2 元群，分别为

$$G_{21}=\{1,\ \sigma^2\},\quad G_{22}=\{1,\ \tau\},\quad G_{23}=\{1,\ \sigma^2\tau\}$$

$$G_{24}=\{1,\ \sigma\tau\},\quad G_{25}=\{1,\ \sigma^3\tau\}.$$

它们之间的关系用图式说明如下：



7. 1) 是显然的.

2) 因为 G 中任意元把 K 中 F 的可离元仍然变为可离元，所以它把 L 仍然变为 L，并且它不使 F 中任意元变动. 又 G 的元数是 n_0，而 $(L:F)=n_0$，所以 G 可以看成 L 关于 F 的伽罗瓦群.

3) 显然 G 中不使 K_1 中任意元变动的元也不使 L_1 中任意元变动，反过来，假如 σ 不使 L_1 中任意元变动，$\alpha\in K_1$，$\alpha^{p^k}\in L_1$，由 $\sigma\alpha^{p^k}=\alpha^{p^k}$ 即得 $(\sigma\alpha-\alpha)^{p^k}=0$，于是 $\sigma\alpha=\alpha$. 所以 σ 也不使 K_1 中任意元变动.

4) 假如 $\alpha^p=a\in K_1$，$\alpha_1^p=a$，因为 $(\alpha-\alpha_1)^p=0$，所以 $\alpha=\alpha_1$，这就是说 $x^p=a$ 只有一个 p 重根. 因为 G_1 中任意元把 $x^p=a$ 的零点仍然变为它的零点，因此它不使 α 变动，所以 $\alpha\in K_1$.

5) 因为 G 中不使 $L(G_1)$ 中任意元变动的元，同样也不使 $K(G)$ 中任意元变动，所以 $G(K(G_1))$ 的元数等于 $G(L(G_1))$ 的元数. 但 G 也可以看成 L 关于 F 的伽罗瓦群，并且

$$G(L(G_1))=G_1,\ G(K(G_1))\supseteq G_1,$$

所以 $G(K(G_1))=G_1$.

6) 假定 $\alpha\in K(G(K_1))$，$\alpha^{p^k}\in L(G(K_1))$，因为 $G(K_1)=G(L_1)$，并且 $L(G(K_1))=L(G(L_1))=L_1$，所以 $\alpha^{p^k}\in L_1$，因此 $\alpha\in K_1$.

习 题 6.5

1. 因为 $n\geqslant5$ 时，A_n 是单群，所以 $S_n\supset A_n\supset E$ 是 S_n 的合成群列，但 A_n 不是可换群.

习 题 6.6

2. x^5-4x+2 有三个实根，所以它不能用根号解出。

习 题 7.1

3. 假定 $m>n$，命 v_i 是 V_i 中任意非零的元，$i=1, \cdots, m$. 因为 V 是 n 个 $W_1, \cdots, W_n$ 的直和，所以 $v_1, \cdots, v_m$ 中某元是其余元的线性组合，假定 $v_m=a_1v_1+\cdots+a_{m-1}v_{m-1}$, $a_i\in R$. 那末 V 中元不能一意地表为 $V_1, \cdots, V_m$ 中元的线性组合，这与 V 是 $V_1, \cdots, V_m$ 的直和的假设不合.

4. 因为 $Z_2\begin{pmatrix}2&0\\2&0\end{pmatrix}\supset Z_2\begin{pmatrix}4&0\\4&0\end{pmatrix}\supset\cdots$，所以 Z_2 不满足极小条件。

习 题 7.2

1. Fu_3.

2. 因为 m 不能用质数平方整除时，$Z-(m)$ 中没有异于零的幂零元.

3. 假如 R 的中心的根基不为零，a 是其中一元，那末 Ra 是 R 中非零的幂零左理想子环，这与假设不合.

4. 假定 $L^n=0$，那末 $(L, LR)^n=0$.

5. 假定 $L^2\neq 0$，那末 L 中有元 a 使 $La\neq 0$，因此 $L=La$. 于是 L 中有元 e 使 $ea=a$. 因此 $e^2a=ea$，即 $(e^2-e)a=0$. 假定 $L'=\{b|b\in L, ba=0\}$，那末 L' 是 R 的左理想子环，并且 $L'\subsetneqq L$，但 $e\in L'$，所以 $L'=0$，因此 $e^2=e$. 于是 $Le\neq 0$，所以 $L=Le$.

习 题 7.3

1. 由定理 3 及定理 6 即得.

2. 假如 $L=Re$ 不是极小左理想子环，命 $L=L_1+L_2$, $e=e_1+e_2$. 因为 $e_1=e_1e=e_1^2+e_1e_2$，所以 $e_1^2=e_1$, $e_1e_2=0$. 同样 $e_2^2=e_2$, $e_2e_1=0$. 因此 e 不是本原幂等元.

4. 假定 $R=L_1+\cdots+L_n$，这里 L_i 是 R 的极小左理想子环. L 是 R 的任意左理想子环，同 §5.4 定理 5 一样，我们有 $L=L_1'+\cdots+L_n'$, $L_i'\subseteq L_i$，因为 L_i 是极小，所以 $L_i'=L_i$ 或 $L_i'=0$. 即 L 是 $L_1, \cdots, L_n$ 中某些 L_i 的直和，因此 R 中左理想子环只有 n^2 个，所以 R 满足极小条件. 再假定 N 是 R 的根

基，那末 $N=NR=NL_1+\cdots+NL_n$，但 $NL_i\subseteq L_i$，如果 $NL_i=L_i$，因为 $N^m=0$，所以 $L_i=N^mL_i=0$，这不可，因此 $NL_i=0$，于是 $N=0$。

习　题　7.4

1．由定理 2，§4.9 魏特邦定理及 §3.1 习题 8 即得。

3．因为两个以上体的直和不再成为体。

4．引用定理 3 及 §7.3 习题 2。

习　题　7.5

1．由 $(-a^2)\circ b=0$ 得 $a\circ((-a)\circ b)=(a\circ(-a))\circ b=(-a^2)\circ b=0$。

2．因为 $\bar{R}=R-J$，所以 $(\bar{R}\bar{x})^2=\bar{R}\bar{x}\bar{R}\bar{x}=0$，即 $\bar{R}\bar{x}$ 是 $\bar{R}$ 的幂零左理想子环，但 $\bar{R}$ 是半单纯环，所以 $\bar{x}=0$，因此 $x\in J$。

3．由 $RaR\in J$ 得 $RaRa=(Ra)^2\in J$，即 $\bar{R}\bar{a}^2=0$，因为 $\bar{R}=R-J$ 是半单纯环，所以 $\bar{a}=0$，于是 $a\in J$。

4．假定 $ab+c+cab=0$，那末 $ba+(-ba-bca)+(-ba-bca)ba=-b(c+ab+cab)a=0$。

5．因为 $-a\in J$，所以 $-a+a'-a'a=0$，于是 $0=(-a+a'-a'a)x=-ax+a'x-a'ax=-x+a'x-a'x=-x$。

6．假定 $L=R$，那末在 R 中有元 a' 使 $a=a'+a'a$，即 $a+(-a')+(-a')a=0$，所以 a 是左拟正则元。再假如 a 是左拟正则元，$a+a'+a'a=0$，因此 $a=(-a')+(-a')a$，所以 $a\in L$。因为对 R 中任意元 r，我们有 $r+ra\in L$，但 $ra\in L$，所以 $r\in L$，即 $R\subseteq L$，因此 $R=L$。

8．因为 $r-re\in L$，显然 $e\notin L$，否则 $r\in L$，即 $R=L$，这不可，于是根据冲恩引理，R 中有包含 L 而不包含 a 的极大左理想子环，这子环又是 R 的极大左理想子环，因为它是 L 的扩张环，所以它又是正则的。

9．由上题及定理 8 即得。

10．假如 $\frac{n}{m}+\frac{n'}{m'}+\frac{n'n}{m'm}=0$，那末 $nm'+n'(m+n)=0$，即 $\frac{n'}{m'}=\frac{-n}{m+n}$，因为 n 是偶数，所以只有 $\frac{2k}{m}$ 是左拟正则元。

11．假定 $x\in N$，如果 $1+x\in N$，那末 $1\in N$，这与假设不合。所以 $1+x$ 有逆元，即 $(1+x)(1+x')=1$，因此 x 是左拟正则元，于是 N 是拟正则理想子环，所以 $N\subseteq J$。再假如 J 中元有逆元，那末 $1\in J$，但 1 不是左拟正则元，所

以 J 中元都是没有逆元的元. 因此 $J\subseteq N$. 于是 $J=N$.

12. 因为 $eJe\subseteq J$, 所以 eJe 中任意元 ere 是 R 的左拟正则元, 即 $ere+b+bere=0$, 因此 $ere+ebe+ebe\cdot ere=0$. 所以 eRe 的根基 $J'\supseteq eJe$. 再假如 $ere\in J'$, 那末 $eRe(ere)$ 是 eRe 的拟正则左理想子环, 于是对于 R 中任意元 x, $exere$ 是左拟正则元, 因此 $xere$ 也是左拟正则元, 所以 $ere\in J$. 于是 $ere\in eJe$, 即 $J'\subseteq eJe$. 因此 $J'=eJe$.

习 题 7.6

1. 因为可换本原环是体.

习 题 7.7

3. 假设 R 是本原环, A, B 是 R 的两个理想子环, 如果 $AB=0$, $B\neq 0$, 因为 R 是 V 的稠密环, 所以 R 中只有零元零化 V. 因此 $BV\neq 0$, 于是 $BV=V$. 所以 $AV=ABV=0$, 所以 $A=0$.

5. 因为 $e\neq 0$, 所以 eV 关于 D 的维数 $\geqslant 1$. 假定 ex, ey 是两个线性无关的元, 根据密度定理, R 中有元 a 使 $aex=0$, $aey\neq 0$. 因此 $ae\neq 0$. 命 $L_x=\{b\in R\,|\,bx=0\}$, 那末 L_x 是 R 的左理想子环, 因为 $ae\in L_x$, $ae\in L$, 而 L 是极小, 所以 $L=L_x$. 因此 $e\in L_x$ 即 $ex=0$. 这与假设不合, 所以 eV 关于 D 的维数是 1.

名词索引

（以汉字笔划为序）

一画

三画

四画

五画

六　画

七　画

八 画

九　画

十　画

十一画

十 二 画

十 三 画

十 四 画

十 五 画

十六画

霍布金斯定理 271

十八画